NETWORK SECURITY USING INTRUSION DETECTION & PREVENTION SYSTEM INTEGRATION MODEL

O.B. Lawal
Computer Science Department,
Olabisi Onabanjo University Consult, Ibadan, Nigeria
E-mail: lawal5@yahoo.com

[1]Corresponding Author

ABSTRACT

Computer networks are now necessities of modern organisations and network security has become a major concern for them. Intrusion Detection Systems (IDS) are increasingly a key part of system defence. Various approaches to Intrusion Detection (ID) are currently being used but they are relatively ineffective when used in isolation. Also, numerous other threats have emerged recently that are particularly troublesome, hence, some solution must be provided to encounter the new generation of complex threats. Building up this solution requires the integration of different security devices and technologies. This study proposed an integration model of combining different intrusion detection and prevention system (IDPS) technologies together with other technologies with IDPS capabilities for systems security and provide guide to integrate the multiple IDPS technologies. This integrated approach allows systems managers to make more informed decisions regarding intrusion detection.

Keywords: Intrusion detection system, Multiple IDPS, Integration, IDPS Technologies .

1. INTRODUCTION

The dramatic growth of the Internet and other computer networks has been accompanied by a significant increase in network intrusions and attacks on computer systems. Given the enormous dependence of both individuals and organizations on information networks, including the Internet, it is important to develop cost-effective measures to mitigate this threat [1]. Not only do we need to quickly and efficiently detect network intrusions and attacks, but we should also have the most appropriate defences if and when a computer system is attacked, since experience shows that there will inevitably be some attacks that either escape detection or cause damage in spite of being detected [1].

An Intrusion Detection System (IDS) device is passive, watching packets of data traverse the network from a monitoring port, comparing the traffic to configured rules and setting off an alarm if it detects anything suspicious. An IDS can detect several types of malicious traffic that would slip by a typical firewall, including network attacks against services; data-driven attacks on applications; host-based attacks such as unauthorized logins; and malware such as viruses, Trojan horses and worms. Most IDS products use several methods to detect threats, usually signature-based detection, anomaly-based detection and stateful protocol analysis [2]. An Intrusion Protection System (IPS) has all the features of a good IDS but can also stop malicious traffic from invading the enterprise.

Unlike an IDS, an IPS sits in-line with traffic flows on a network, actively shutting down attempted attacks as they're sent over the wire. It can stop the attack by terminating the network connection or user session originating the attack; by blocking access to the target from the user account, IP address or other attribute associated with that attacker; or by blocking all access to the targeted host, service or application [2]. Layered security is the key to protecting any size network. For most companies, that means adding both IDS and IPS products to the network. When it comes to IPS and IDS, it's not a question of which technology to add to your security infrastructure – both are required for maximum protection against malicious traffic. In fact, vendors are increasingly combining the two technologies into a single box [2].

Organizations should consider using multiple types of IDPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity [3]. The four primary types of IDPS technologies— network based, wireless, NBA, and host-based— each offer fundamentally different information gathering, logging, detection, and prevention capabilities. Each technology type offers benefits over the others, such as detecting some events that the others cannot and detecting some events with significantly greater accuracy than the other technologies. In many environments, a robust IDPS solution cannot be achieved without using multiple types of IDPS technologies [3].

For most environments, a combination of network-based and host-based IDPS technologies is needed for an effective IDPS solution. Wireless IDPS technologies may also be needed if the organization determines that its wireless networks need additional monitoring or if the organization wants to ensure that rogue wireless networks are not in use in the organization's facilities. NBA technologies can also be deployed if organizations desire additional detection capabilities for denial of service attacks, worms, and other threats that NBAs are particularly well-suited to detecting.

Organizations should consider the different capabilities of each technology type along with other cost-benefit information when selecting IDPS technologies [3]. The model and approach presented in this paper allows us to analyse the performance of an IDS. It also helps us to analyse the state of the system if an attack goes through. The synergistic advantage of this approach is that improvements in the performance of the IDS can be directly incorporated into survivability estimation. In general, a systems manager would like to manage both the security as well as the investment for that security. The integration (hybrid) model we propose has the potential to lead to a Decision Support System (DSS) that could help systems managers make more informed decisions about the IDSs for their sites and about the kind of protection their systems should have.

The structure of the rest of the paper is as follows. Section 2 discusses prior and related works while section 3 gives an insight to the intrusion detection system. In section 4, guide to integrate multiple IDPS technologies were presented. Section 5 presents the benefits of integration multiple IDPS technologies. In section 6, conclusion to the study is presented.

2. RELATED WORK

Here, the study present woks that has been done up to now in the area of Integrity of various security tools and correlating the events from the integrated tools and integrating multiple solutions for network security.

There are two broad techniques for network security: protection and detection [5]. The protection technique tries to protect the system from attack. The most commonly used protection device is the firewall which allows only valid data to pass through it. Another approach is using an IDS, which collects information from a variety of systems and network sources, and analyses the data stream for signs of intrusion or misuse. The modelling of an IDS has always been an important problem for researchers in this area. [1] proposed an IDS model based on historical data and [6] provides a detailed survey of the work done on this topic. The success of an IDS is measured by the false positives and the true positives.

YING-DAR LIN, et al [6] discusses how the integrated security gateway can be implemented using the open source packages. These open source packages ensure the interoperability between the packages. Glenn A. Fink, Paul Muessig, and Chris North [7] introduces Portall, visualization tool that gives system administrators a view of the communicating processes on the monitored machine correlated with the network activity in which the processes participate [7].

Ron Gula [8] presents the vulnerability correlation with the IDS alerts and specifies two methods of correlating the vulnerability with the IDS alerts. These are Persistent VA/IDS Correlation and near time VA/IDS Correlation. NetForensics [7] integrates three distinct yet complimentary forms of event correlation – the first is rules based correlation which separates false positive security alarms from potentially significant security incidents by invoking "time aware" security policy rules for each event received from IDS, OS, APPS, or AVS devices monitored by netForensics.

The second is Statistical Correlation and third one is Vulnerability correlation. Robert Ball, Glenn A. Fink, Anand Rathi, Sumit Shah, and Chris North [7] explains a tool named VISUAL (Visual Information Security Utility for Administration Live) that provides insight for networks with up to 2,500 home hosts and 10,000 external hosts, shows the relative activity of hosts, displays them in a constant relative position, and reveals the ports and protocols used [7]. Tarun Bhaskar proposed a holistic approach to network security with a hybrid model that includes an Intrusion Detection System (IDS) to detect network attacks and a survivability model to assess the impacts of undetected attacks. A neural network-based IDS has been proposed, where the learning mechanism for the neural network is evolved using genetic algorithm. Then the case where an attack evades the IDS and takes the system into a compromised state was discussed [1].

3. INTRUSION DETECTION SYSTEMS

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices [3]. According to [7], an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization [7].

Many network intrusions cannot be identified until the traffic has been passively analyzed. For example, denial of service (DoS) attacks such as ICMP-flooding are difficult to recognize until numerous ICMP packets have arrived within a small time interval; application-specific buffer overflow attacks to obtain root privilege, such as subverting an FTP server by a long “MKDIR” command, may require buffering and reassembling several packets before seeing the whole FTP command [7]. A network-based IDS can detect such attacks by matching a sub-string, for example, the “phf” in “ GET/cgi-bin/phf?,” to identify those network packets as vehicles of a web server attack. When such kinds of potential hostile activities are detected, IDS will alert system administrators and may block the activity. The above examples describe the basic functions of a network based IDS [7].

In fact, the IDS model can be host-based IDS (HIDS) or network-based IDS (NIDS). HIDS is installed at a host to periodically monitor specific system logs for patterns of intrusions. In contrast, an NIDS sniffs the traffic to analyze suspicious behaviors. A *signature-based* NIDS (SNIDS) examines the traffic for patterns of known intrusions. NIDS can quickly and reliably diagnose the attacking techniques and security holes without generating an over-whelming number of false alarms because SNIDS relies on known signatures. However, *anomaly-based* NIDS (ANIDS) detects unusual behaviors based on statistical methods. ANIDS could detect symptoms of attacks without specific knowledge of details. However, if the training data of the normal traffic are inadequate, ANIDS may generate a large number of false alarms [7]. The four primary types of IDPS technologies (network-based, wireless, network behaviour analysis (NBA), and host-based), each offer fundamentally different information gathering, logging, detection, and prevention capabilities [3]. Each technology type offers benefits over the other, such as detecting some events that the others cannot, detecting some events with significantly greater accuracy than the other technologies, and performing in-depth analysis without significantly impacting the performance of the protected hosts [3].

3.1 Types of IDPS Technologies

There are many types of IDPS technologies, which are differentiated primarily by the types of events that they can recognize and the methodologies that they use to identify incidents [3] [8]. For the purposes of this paper, they are divided into the following four groups based on the type of events that they monitor and the ways in which they are deployed [3] as state below:

i. Network-Based, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity [3]. It can identify many different types of events of interest. It is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks.

ii. Wireless, which monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves. It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring. It is most commonly deployed within range of an organization’s wireless network to monitor it, but can also be deployed to locations where unauthorized wireless networking could be occurring [9] in [3].

iii. Network Behaviour Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems) [9]. NBA systems are most often deployed to monitor flows on an organization’s internal networks, and are also sometimes deployed where they can monitor flows between an organization’s networks and external networks (e.g., the Internet, business partners’ networks).

iv. Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Examples of the types of characteristics a host-based IDPS might monitor are network traffic (only for that host), system logs, running processes, application activity, file access and modification, and system and application configuration changes. Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information [3]. Some forms of IDPS are more mature than others because they have been in use much longer [3]. Network-based IDPS and some forms of host-based IDPS have been commercially available for over ten years [3]. Network behaviour analysis software is a somewhat newer form of IDPS that evolved in part from products created primarily to detect DDoS attacks, and in part from products developed to monitor traffic flows on internal networks. Wireless technologies are a relatively new type of IDPS, developed in response to the popularity of wireless local area networks (WLAN) and the growing threats against WLANs and WLAN clients [3].

4. GUIDE TO INTEGRATE MULTIPLE IDPS TECHNOLOGIES

Combining and integrating different IDPS technologies are also required and therefore recommended to ensure sound network security for large organisations. Accordingly, organizations should consider using multiple types of IDPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity, with lower rates of false positives and false negatives [3]. This section provides guidance on using multiple IDPS technologies to create a broader IDPS solution and discusses the advantages and disadvantages of using multiple technologies. Organizations that are planning to use multiple types of IDPS technologies, or even multiple products within a single IDPS technology class, should consider whether or not the IDPS products should be integrated in some way, either working together directly or feeding their data into a centralized logging system or security information and event management system [3]. This section explains how different IDPS products can be integrated, and the benefits and limitations of the integration methods. It also provides overviews of other technologies that complement IDPS technologies with how they can be included in an IDPS solution to further improve detection and prevention.

4.1 The Need for Multiple IDPS Technologies

In many environments, a robust IDPS solution cannot be achieved without using multiple types of IDPS technologies [3]. For example, network-based IDPSs cannot monitor wireless protocols, and wireless IDPSs cannot monitor application protocol activity. Table 4-1 provides a high-level comparison of the four primary IDPS technology types. The strengths listed in the table indicate the roles or situations in which each technology type is generally superior to the others. A particular technology type may have additional benefits over others, such as logging additional data that would be useful for validating alerts recorded by other IDPSs, or preventing intrusions that other IDPSs cannot because of technology capabilities or placement (e.g., on the host instead of on the network) [10].

Table 4-1 Comparison of IDPS Technology Types [11]

IDPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor or Agent	Strengths
Network-Based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Able to analyze the widest range of application protocols; only IDPS that can thoroughly analyze many of them
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WLANs and groups of wireless clients	Only IDPS that can monitor wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections
Host-Based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity	Individual host	Only IDPS that can analyze activity that was transferred in end-to-end encrypted communications

For most environments, a combination of network-based and host-based IDPSs is needed for an effective IDPS solution. Wireless IDPSs may also be needed if the organization determines that its wireless networks need additional monitoring or if the organization wants to ensure that rogue wireless networks are not in use in the organization's facilities. NBA products can also be deployed if organizations desire additional detection capabilities for denial of service (DoS) attacks, worms, and other threats [11].

In addition to using multiple types of IDPS technologies, some organizations also use multiple products of the same IDPS technology type [11]. This is often done to improve detection capabilities. Because each product uses somewhat different detection methodologies and detects some events that another product cannot, using multiple products can allow for more comprehensive detection of possible incidents. Also, having multiple products in use, particularly to monitor the same activity, makes it easier for analysts to confirm the validity of alerts and identify false positives, and also provides redundancy, should one product fail for any reason [11].

4.2 Integrating Different IDPS Technologies

Many organizations use multiple IDPS products, usually from different vendors (most vendors make products in only one IDPS technology type). By default, these products function completely independently of each other. This has some notable benefits, such as minimizing the impact that a failure or compromise of one IDPS product has on other. IDPS products. However, if the products are not integrated in any way, the effectiveness of the entire IDPS implementation may be somewhat limited. Data cannot be shared by the products, and IDPS users and administrators may have to expend extra effort to monitor and manage multiple sets of products [12]. IDPS products can be directly integrated, such as one product feeding alert data to another product, or they can be indirectly integrated, such as all the IDPS products feeding alert data into a security information and event management system. Sections 4.2.1 and 4.2.2 discuss the benefits and limitations of direct and indirect integration, respectively.

4.2.1 Direct IDPS Integration

Direct IDPS integration is most often performed when an organization uses multiple IDPS products from a single vendor [11]. For example, some vendors offer both network-based and host-based products. These vendors frequently offer a single console that can be used to manage and monitor both types of products. This can provide significant time savings to administrators and users because it streamlines their work. Some products also share data; for example, a product might use host-based IDPS data to determine if an attack detected by network-based IDPS sensors was successful, or if an attack stopped by network-based IDPS data would have been successful if allowed to pass. This information can speed the analysis process and help users to better prioritize threats. The primary disadvantage of using a fully integrated solution is that a failure or compromise could endanger all the IDPS technologies that are part of the integrated solution [11].

A more limited form of direct IDPS integration is having one IDPS product provide data for another IDPS product [12]. As mentioned previously, two products from the same vendor often share data with each other for correlation purposes. Data can also be shared among products from different vendors [11], although typically this simply involves one product providing data as input to the second product [12]. For example, a network-based IDPS could potentially provide network flow information to an NBA sensor. A host-based IDPS could provide system configuration information to NBA or network-based IDPS sensors. This data can be used for event correlation and better prioritization of alerts.

4.2.2 Indirect IDPS Integration

Indirect IDPS integration is usually performed with security information and event management (SIEM) software [13]. SIEM software is designed to import information from various security-related logs and correlate events among them [13]. Log types commonly supported by SIEM software include IDPSs, firewalls, antivirus software, and other security software; OSs (e.g., audit logs); application servers (e.g., Web servers, e-mail servers); and even physical security devices such as badge readers.

SIEM software generally works by receiving copies of the logs from the logging hosts over secure network channels, converting the log data into standard fields and values (known as *normalization*), then identifying related events by matching IP addresses, timestamps, usernames, and other characteristics. SIEM products can identify malicious activity such as attacks and malware infections, as well as misuse and inappropriate usage of systems and networks. Some SIEM software can also initiate prevention responses for designated events. SIEM products usually do not generate original event data; instead, they generate meta-events based on their analysis of the imported event data [12].

How SIEM software complements IDPSs include the following:
- SIEM software can identify some types of events that individual IDPSs cannot because of its ability to correlate events logged by different technologies [11].
- The consoles for SIEM software can make data from many sources available through a single interface, which can save time for users that need to monitor multiple IDPSs. SIEM consoles also may offer analysis and reporting tools that certain IDPSs' consoles do not.
- Users can more easily verify the accuracy of IDPS alerts because the SIEM may be able to link each alert to supporting information from other logs. This can also help users to determine whether or not certain attacks succeeded [11].

Limitations of SIEM software in the context of IDPS include the following:
- There is often a considerable delay between the time an event begins and the time the SIEM sees the corresponding log data. Log data may be transferred from logging hosts to the SIEM in batch mode, such as every 5 or 10 minutes. As a result, malicious activity alerts are often displayed on an IDPS console earlier than on a SIEM console, and prevention actions are less timely [12].
- SIEM products typically transfer only some data fields from the original logs. For example, if a network-based IDPS records packets, the packets may not be transferred to the SIEM because of bandwidth and storage limitations. Also, the log normalization process that converts each data field to a standard format and labels the data consistently can occasionally introduce errors in the data or cause some data to be lost. Fortunately, SIEM products typically do not alter the original data sources, so they can be referenced to verify the accuracy of the data if needed [11].

- SIEM software may not offer agents for all IDPS products. This could require administrators to write custom agents to transfer IDPS data to the SIEM servers, or it could necessitate having the IDPSs perform logging using a different mechanism so that the SIEM software can understand the log format [12].

An alternative to using SIEM software for centralized logging is to use a solution based primarily on the syslog protocol [13]. Syslog provides a simple framework for log generation, storage, and transfer that any IDPS could use if designed to do so. Some IDPSs offer features that allow their log formats to be converted to syslog format [13]. Syslog is very flexible for log sources, because each syslog entry contains a content field into which logging sources can place information in any format. However, this flexibility makes analysis of the log data challenging.

Each IDPS may use many different formats for its log messages, so a robust analysis program would need to be familiar with each format and be able to extract the meaning of the data within the fields of each format. It might not be feasible to understand the meaning of all log messages, so analysis might be limited to keyword and pattern searches. Generally, the use of syslog for centralized collection and analysis of IDPS logs does not provide sufficiently strong analysis capabilities to support incident identification and handling [13].

4.3 Other Technologies with IDPS Capabilities

In addition to dedicated IDPS technologies, organizations typically have several other types of technologies that offer some IDPS capabilities and complement the primary IDPSs [11]. This section discusses common types of complementary technologies: network forensic analysis tools, anti-malware technologies (antivirus software and antispyware software), firewalls and routers, and honeypots.(NIST) For each, a brief overview of the technology is provided, and its use in intrusion detection and prevention and its relationship to IDPSs are explained. Recommendations are also made as applicable for how the complementary technologies should be used alongside of IDPSs.

4.3.1 Network Forensic Analysis Tool (NFAT) Software

Network forensic analysis tools (NFAT) focus primarily on collecting and analyzing wired network traffic [11]. Unlike a network-based IDPS, which performs in-depth analysis and stores only the necessary network traffic, an NFAT typically stores most or all of the traffic that it sees, and then performs analysis on that stored traffic. In addition to its forensic capabilities, NFAT software also offers features that facilitate network traffic analysis, such as the following:

- Reconstructing events by replaying network traffic within the tool, ranging from an individual session (e.g., instant messaging [IM] between two users) to all sessions during a particular time period. The speed of the replaying can typically be adjusted as needed [11].
- Visualizing the traffic flows and the relationships among hosts. Some tools can even tie IP addresses, domain names, or other data to physical locations and produce a geographic map of the activity.
- Building profiles of typical activity and identifying significant deviations.
- Searching application content for keywords (e.g., “confidential”, “proprietary”).

This makes it more valuable for network forensics and less valuable for intrusion detection and prevention than a typical network-based IDPS [11].

Ways in which NFAT software complements IDPSs include the following:

- NFAT software is often more valuable for network forensics than IDPS software because of its extensive packet logging.
- Having NFAT software perform packet logging can reduce the load on network-based IDPS sensors.
- NFAT software might be better-suited to customization, especially for content searches (e.g., keywords), than some IDPS technologies.
- Some NFAT graphical user interfaces (GUI) may offer analysis, visualization, and reporting capabilities that IDPS consoles do not.

Limitations of NFAT software in the context of IDPS include the following:

- NFAT software usually does not have the intrusion detection capabilities of network-based IDPSs.
- NFAT software typically offers no intrusion prevention capabilities.

4.3.2 Anti-Malware Technologies

The most commonly used technical control for malware threat mitigation is antivirus software. Types of malware that it can detect include viruses, worms, Trojan horses, malicious mobile code, and blended threats, as well as attacker tools such as keystroke loggers and backdoors. Antivirus software typically monitors critical OS components, filesystems, and application activity for signs of malware, and attempts to disinfect or quarantine files that contain malware. Most organizations deploy antivirus software both centrally (e.g., e-mail servers, firewalls) and locally (e.g., file servers, desktops, laptops) so that all major malware entry vectors can be monitored [11].

Another commonly used control for malware threat mitigation is spyware detection and removal utilities, also known as antispyware software. They are similar to antivirus software, but they focus on detecting both malware and non-malware forms of spyware, such as malicious mobile code and tracking cookies, and spyware installation techniques such as unauthorized Web browser plug-in installations, popup ads, and Web browser hijacking [11].

Both antivirus and antispyware products detect threats primarily through signature-based analysis. To identify previously unknown threats, they also use heuristic techniques that examine activity for certain suspicious characteristics. The product vendors create and release additional signatures when new threats emerge, so that the products can detect them.

Ways in which antivirus and antispyware software complements IDPSs include the following:

- IDPSs usually have limited malware and spyware detection capabilities (often only for the most common threats, such as widespread worms), so antivirus and antispyware software can detect many threats that IDPSs cannot [11].
- NBA technology might identify that a worm is spreading based on unusual traffic flows, but it probably could not identify which worm it is. Antivirus software should be able to determine which worm it is, if the threat is not a new one for which the antivirus software does not yet have signatures.
- Antivirus software, and to a lesser extent antispyware software, can take some load from IDPSs, such as having antivirus software identify instances of a particular worm and disabling the worm's signatures on the IDPS sensors. This is particularly important during a widespread malware infection, when IDPSs might become overwhelmed with worm alerts and other important events occurring at the same time might go unnoticed by IDPS users [11].

Limitations of antivirus and antispyware software in the context of IDPS include the following:

- Antivirus and antispyware software cannot detect threats other than malware and spyware.
- Network-based IDPS and NBA software are often better able to recognize network service worms than antivirus software can because antivirus software often monitors only the most common application protocols. Also, antispyware software typically cannot detect network service worms. Network-based IDPS and NBA software can typically monitor any protocol [11].
- For a new threat, antivirus and antispyware software often cannot recognize it until the vendor releases new signatures and updates are installed. In some cases, especially for threats with easily identifiable characteristics, an IDPS can detect the new threat during this window of time because IDPS administrators can write a custom signature for the IDPS. Antivirus and antispyware software typically do not permit administrators to write signatures. Also, NBA software can often recognize new worms by their anomalous traffic patterns [11].

4.3.3 Firewalls and Routers

Firewalls (network-based and host-based) and routers filter network traffic based on TCP/IP characteristics such as the source and destination IP addresses, the transport layer protocol (e.g., TCP, UDP, ICMP), and basic protocol information (e.g., TCP or UDP port numbers, ICMP type and code). Most firewalls and routers log which connections or connection attempts they block; the blocked activity is often generated by unauthorized access attempts from automated attack tools, port scanning, and malware. Some network-based firewalls also act as proxies. When a proxy is used, each successful connection attempt actually results in the creation of two separate connections: one between the client and the proxy server, and another between the proxy server and the true destination. Many proxies are application-specific, and some actually perform some analysis and validation of common application protocols, such as HTTP. The proxy may reject client requests that appear to be invalid (which could include some forms of attacks) and log information regarding these requests [11].

Ways in which firewalls and routers complement IDPSs include the following:

- Network-based firewalls and routers often perform network address translation (NAT), which is the process of mapping addresses on one network to addresses on another network. NAT is most often accomplished by mapping private addresses from an internal network to one or more public addresses on a network that is connected to the Internet. Firewalls and routers that perform NAT typically record each NAT address and mapping. IDPS users may need to make use of this mapping information to identify the actual IP address of a host behind a device performing NAT [11].

- If IDPSs and other security controls (e.g., antivirus software) cannot stop a new network-borne threat, such as a network service worm or denial of service attack, firewalls or routers might have to be temporarily reconfigured to block the threat.
- Many IDPSs can reconfigure firewalls or routers to block particular threats.
- Routers are often used as data sources for NBA deployments.

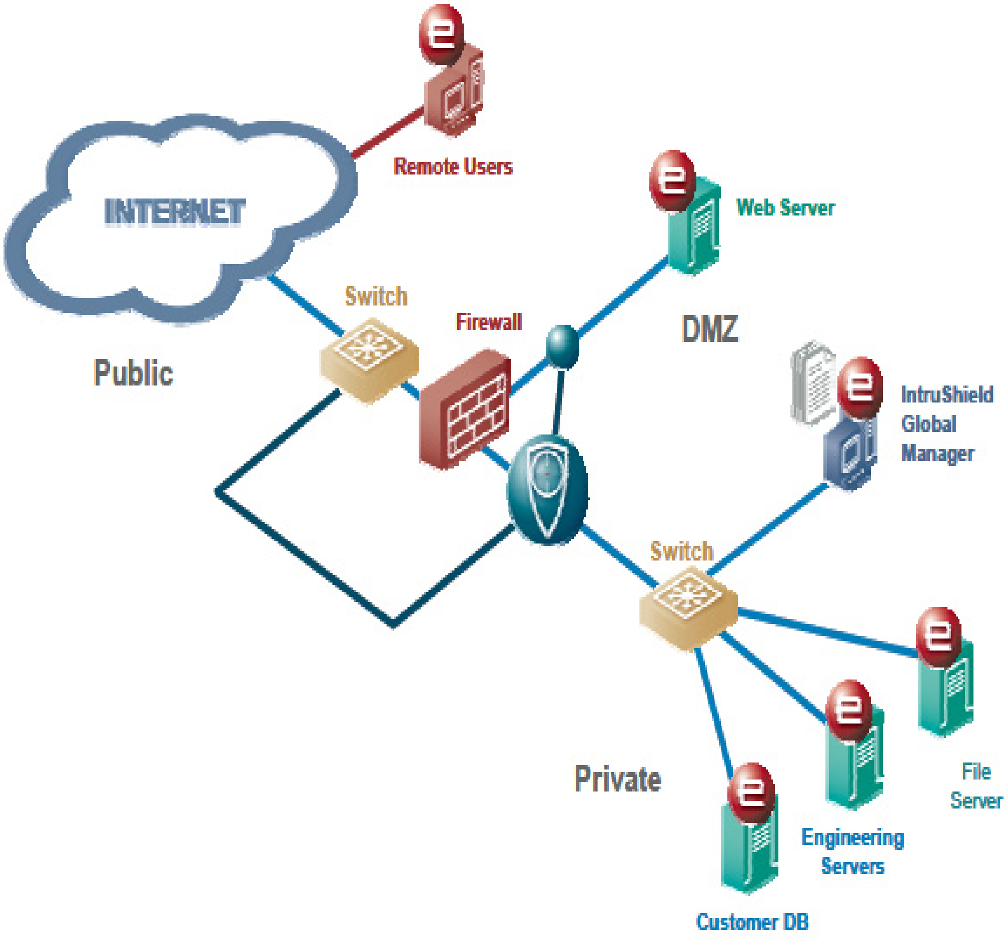
***Limitations of firewalls and routers in the context of IDPS include the following*:**

- Firewalls and routers cannot detect most types of malicious activity.
- Firewalls and routers typically log relatively little information, such as the basic characteristics of denied connection attempts only, and they rarely record the content of any packets. NBA technologies and some network-based IDPSs can log much more information about network traffic than firewalls and routers do [11].

4.3.4 Honeypots

Some organizations are sufficiently concerned with detecting the earliest signs of widespread incidents, such as major new worms, that they deploy deceptive measures such as honeypots so that they can collect better data on these threats [15]. Honeypots are hosts that have no authorized users other than the honeypot administrators because they serve no business function; all activity directed at them is considered suspicious. Attackers will scan and attack honeypots, giving administrators data on new trends and attack tools, particularly malware. However, honeypots are a supplement to, not a replacement for, other security controls such as intrusion detection and prevention systems.

If honeypots are to be used by an organization, qualified incident handlers and intrusion detection analysts should manage them. The legality of honeypots has not been clearly established; therefore, organizations should carefully study the legal ramifications before planning any honeypot deployments [15].



Integrated IPS Deployment [16]

5. IMPACTS OF INTEGRATING MULTIPLE IDPS TECHNOLOGIES

1. Combining “Best of Breed” Host and Network IPS technology results in a more comprehensive and robust defensive posture, meaning fewer successful attacks, more efficient use of scare security resources and lower operating costs than simply deploying one technology or the other.
2. An intrusion or compromise consists of multiple stages: Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Clearing Tracks. Although both Host and Network IPS have the ability to prevent each stage, both technologies are not equally adept at detecting and blocking each stage. Integrating the strengths of each architecture provide a solution whose sum is greater than its parts. By deploying complementary, integrated “Protection-in-Depth” technologies such as McAfee Network and Host IPS, organizations can achieve superior protection at a reasonable cost.
3. By providing proactive security at a network’s most vulnerable points, IDPS integration protects organization from the many deleterious effects of succumbing to a security attack – data loss, wasted time, loss of business availability and a damaged reputation [16].

4. Companies that deploy an integrated IDPS model also gain help in maintaining regulatory compliance.

5. An IDPS device is helpful beyond the attacks it stops and the reports it logs. An IDPS can take the place of specialized security personnel a company can’t afford to retain. The automated interdiction capabilities of an IDPS device make it easier to consistently enforce a security policy, showing compliance with stated security policies when audit time rolls around [16].

6. CONCLUSION

In this paper, the capabilities of the major IDPS (Network-Based, Wireless, Network Behaviour Analysis, Host-Based) were analysed and some other technologies with IDPS capabilities (i.e. network forensic analysis tools, anti-malware technologies, Firewalls and Routers and honeypots) in a way to combine them to enforce security on the network. Integrating different IDPS technologies requires a guide to follow which were therefore recommended to ensure sound network security for large organisations having in mind the values of their resources. With the combination and integrated measures on networks, Systems and Network Administrators (Managers) can ensure safer and secured organisational resources from attacker and intruders, and also lead to a Decision Support System that could help systems managers make more informed decisions about the IDSs for their sites and about the kind of protection their systems should have.

REFERENCES

[1] Tarun Bhaskar et al. A Hybrid Model for Network Security Systems: Integrating Intrusion Detection System with Survivability. International Journal of Network Security, Vol.7, No.2, PP.249–260, Sept. 2008.

[2] IDS IPS Buyer's Guide. IT Security. Available at www.itsecurity.com

[3] O.B. Lawal, A. Ibitola & O.B. Longe (2013). Analysis and Evaluation of Network-Based Intrusion Detection and Prevention System in an Enterprise Network Using Snort Freeware. Afr J. of Comp & ICTs. Vol 6, No. 1. Pp 169-184

[4] T. F. Lunt, "A survey of intrusion detection techniques," Computer and Security, vol. 12, no. 4, pp. 405-418, 1993.

[5] Ying-Dar Lin, Huan-Yunwei, and ShaoTangYu, Building an Integrated Security Gateway:Mechanisms performance Evaluations, Implementations and Research Issues, EEE communications Survey, the electronic Magazine of original peer reviewed survey articles. http://www.comsoc.org/pubs/surveys.

[6] Yudhvir Singh, Yogesh Chaba, Prabha Rani. Integrating – VPN and IDS – An approach to Networks Security International Journal of Computer Science and Security, Volume (1): Issue (3). 2002.

[7] Ron Gula, Correlating IDS Alerts with Vulnerability Information, Tenable Network Security http://www.tenablesecurity.com (December 2002).

[8] Northcutt, Stephen and Novak, Judy, Network Intrusion Detection: An Analyst's Handbook, Third Edition, New

[9] Bace, Rebecca, *Intrusion Detection*, Macmillan Technical Publishing, 2000.

[10] Bejtlich, Richard, *The Tao of Network Security Monitoring: Beyond Intrusion Detection*, Addison-Wesley, 2004.

[11] NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), *Recommendations of the National Institute of Standards and Technology by* Karen Scarfone & Peter Mell, 2007.

[12] NIST SP 800-92, *Guide to Computer Security Log Management*, available at http://csrc.nist.gov/publications/nistpubs/

[13] *The BSD Syslog Protocol*, http://www.ietf.org/rfc/rfc3164.txt.

[14] William Stallings & Lawrie Brown. Computer Security: Principles and Practice. Published Aug 2, 2007 by Prentice Hall. ISBN-13: 978-0-13-600424-0. 1st Edition

[15] SANS Institute InfoSec Reading Room. Honey Pots and Honey Nets - Security through Deception by William W. Martin. SANS Institute 2003

[16] McAfee Security White Paper on Host and Network Intrusion Prevention. Competitors or Partners? June 2004.

Author's Brief

Babatunde O. Lawal is a lecturer in Computer Science at the Olabisi Onabanjo University Consult, Ibadan, Nigeria. He received his Master of Computer Systems (MCS) degree from University of Ibadan, Nigeria. He has worked for Trans International Bank as IT Support Officer and Database Administrator. His research interests are Database Management, Data Mining, Information Systems Management and Network Security. He can be reached at lawal5@yahoo.com.