International Journal of Engineering & Technology, 7 (4.15) (2018) 55-58

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Comparative Study of Traditional and Next Generation IPS

Mohammed Nadir Ali[1], Madihah Mohd Saudi[2,3]*, Touhid Bhuiyan[1], Azreena Abu Bakar[2]

[1]Daffodil International University, Dhaka, Bangladesh
[2]Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Malaysia
[3]CyberSecurity and Systems Research Unit, Islamic Science Institute (ISI), Universiti Sains Islam Malaysia (USIM), Malaysia
**Corresponding author E-mail: madihah@usim.edu.my*

Abstract

Currently, cyber threats and attacks become a main concern among Internet users. To detect and prevent new and unknown attacks, an intelligent intrusion prevention system (IPS) which is better compared with traditional systems is needed. Furthermore, the Next Generation Intrusion Prevention System (NIGPS) is more suitable that could provide an intelligent IPS solution for new and unknown attacks. Therefore, this paper presents the limitation of traditional IPS systems, a comparison between IPS and NIGPS and proposes an enhanced model for NIGPS.

Keywords: *Detection; Intrusion Prevention System (IPS); Model; Next Generation Network Intrusion Prevention System (NGIPS).*

1. Introduction

With Next Generation Intrusion Prevention System (NGPIS) is designed to provide wide protection of vulnerabilities, especially at the application layer. It controls the behavior of applications. It also allows access and provides real-time protection. A traditional IPS was designed to identify the known attacks. Traditional IPSs are black boxes that offer little visibility into the protection being offered, but NGIPS will go way beyond the signature-based protection. However, a next-generation IPS includes network security beyond detection and prevention. It has the capability of visibility, custom rules, vulnerability-based protection and is able to analyze the network attack behavior.

The existing technologies are vulnerable to smart cyber-attacks and very limited to guarantee growth and safety of networks. NGIPS offers comprehensive threat security that blocks intrusions and safeguards valuable assets [1]. NGIPS makes use of an innovative multi-layer approach. It helps to figure out known, 0-day, and advanced persistent threats. It also defends network from worms, spyware, malware, Trojan horse, brute force attacks, protocol attacks, and web threats. Many organizations presently allow their employees to use smart devices, such as smartphones, and popular community applications and social networks for work to increase employee productivity.

The growing rate of security incidents suggests that the threat landscape in information security is taking new shape and traditional technologies cannot protect them against the new generation threats. New generation threats are generally 0-day vulnerability-based attacks that concentrate on unique victims. Conventional security technologies are slow to create signatures, hence giving attacks sufficient time to cause excessive harm. Furthermore, attackers might also customize the attack for the target's surrounding which may cause the attack to remain undetected for a long time. The increasing number of attacks proves that obsolete technologies cannot help organizations to protect themselves from new generation attacks. Organizations now need an updated IPS with provisions for improved inbuilt systems to fight away the new challenges and threats in the foreseeable future automatically. The new Generation Intrusion Prevention System (NGIPS) is designed to cope with such unpredictable challenges and cyber threats of the new millennium.

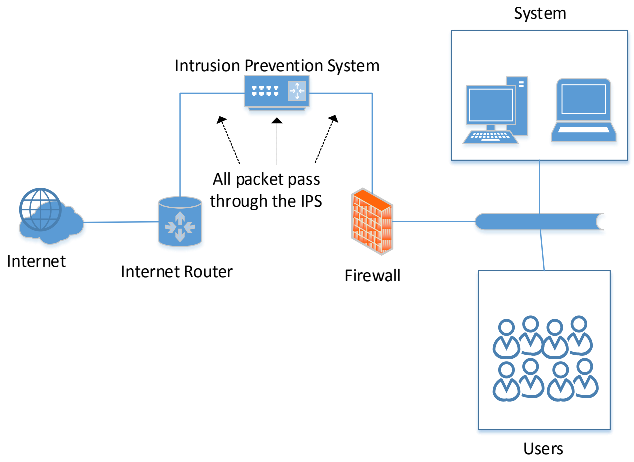

Fig. 1: Basic IPS

Figure 1 shows the basic IPS model. The first commercially available network intrusion detection system was released in the mid 1990's. The current industry perceptions of "next generation" intrusion prevention systems are essentially traditional IPS capabilities with the addition of application and identity awareness [1]. In the Internet world, network security is playing a vital role. A number of tools and devices have already been developed to combat malware attacks or any sort of malicious network activity in order to ensure the computer and network security.

The security frameworks have been constantly changing since the beginning of the journey of the IT. With such continuous systemic changes hackers have been changing their hacking tactics with increasing capabilities. Hence, the new Generation Prevention Systems must keep on guard to cope with unforeseen problems and issues related to cyber security. In order to cope with these continuous changes, the IT sector has also gone through a few phases of its own evaluation, which one may call generation changes in the history of IDS:

- First Generation: The first-generation of IDS was engineered to look for known exploits and warn organizations that an attack may have occurred. First generation systems required research teams to write multiple exploit signatures, which just did not scale.
- Second Generation: In the second-generation IDS solutions, applications changed from exploiting detection to vulnerability detection.
- Third Generation: In the third-generation, it became apparent that signature detection could not be scaled at the required rate to detect malware.
- Fourth Generation (Next Generation): Commonly referred as the "next generation" intrusion prevention system (NGIPS). Products in this category include features such as application and user identity.

The paper is organized as follows: Section 1 covers the introduction and background to the study, Section 2 presents a comparative analysis based on previous works which include the detection, approaches, IPS challenges, mapping the processes of IPS, a comparison between traditional IPS and NGIPS, risk assessment of IPS and working processes of NGIPS. Section 3 presents the proposed model for NGIPS based on the comparative analysis made in Section I2 and Section 4 presents the conclusion of this paper.

2. Comparative Analysis

In the IPS, it is exceptionally hard to distinguish and recognize network traffic in real-time. To identify suspicious threats, there are two popular approaches which are host-based approach and network-based approach. Figure 2 shows the detection method of IPS systems.

Host-based approach is host-based intrusion detection systems that are expected to gather information about activity on a specific single host [2]. These host-based agents which are sometimes referred to as sensors would typically be installed on a machine that is deemed to be susceptible to possible attacks [3]. It checks for suspicious activity from the host or operating system level to monitor location using the agent component before the host reaches its target of attack [4]. Host-based IPS operates by detecting attacks that occur in a host on which it is installed.

Network-based approach involves the deployment of monitoring devices or sensors all through the network to capture and analyse the traffic. Sensors detect malicious and unauthorized activity in real time and can act when required. Sensors are deployed at designated network points that enable security managers to monitor network activity, while it is occurring, regardless of the location of the attack target [5]. The network-based detection provides real-time security insights into the networks.

2.1. Detection Methods

The NIPSs uses one of two detection methods, which are Signature based or Anomaly-based detection [6].

- Signature-Based Detection
  Signatures are attack patterns, which are predetermined and preconfigured [7]. This detection method monitors the network traffic and compares it with the preconfigured signatures to find a match. On successful locating a match, the NIPS takes the next appropriate action. This type of detection fails to identify 0-day error threats. In any case, it has proven to be effective against single packet attacks.

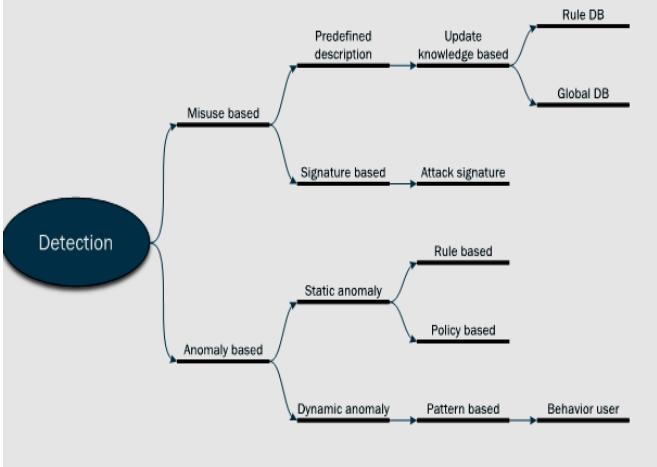

Fig. 2: Detection Methods

- Anomaly-Based Detection
  This method of detection creates a baseline on average network conditions. Once a baseline is created, the system intermittently samples network traffic on the basis of statistical analysis and compares the sample to the baseline. If the activity is found to be outside of the baseline parameters, NIPS takes the necessary action. This anomaly-based detection determines the normal network activities such as determining the bandwidth generally used, type of protocols used, ports and devices generally connected to each other and alerts the system administrator when anomalous traffic is identified [8].

2.2. Challenges of IPS

Nowadays, Internet security is a vital issue in the cyber world. Intrusion detection and prevention system are playing significant roles in this field. It needs intelligent IPS for better accuracy detection rate and faster response. The NGIPS in order to achieve an accurate detection rate and faster response, proposes new effective analysis techniques. New algorithms are proposed on IPS and IDS implementation. However, the rate of attacks increases every day due to the increasing cyber threats and easiness of accessibility of computer devices [9]. The attackers find loopholes to trade off the remote host and utilize it as an instrument for stealing resources from the network [10]. The false positive alarm rate is one of the biggest problems in IPS. In order to monitor and evaluate the alerts, a skilled IPS analyst has to stay on the top of all new attacks, worms, viruses, different operating systems, network changes to keep the network secure. A range of commercial IDS [11] has been developed to detect intrusions with various approaches.

2.3. Mapping Processes of IPS

Figure 3 shows the mapping technique to determine each phase in IPS architecture. It is shown that active response will trigger action (block, allow, logging, report) to mitigate the network connection or the process associated with the event to summarize the four possible cases. Accordingly, TN as well as TP is to identify action sensor, which is labeled as a normal or known activity. On the contrary, FP and FN are the events that undermine the detection performance when an unknown or suspicious user is not identified. These high-level alarms can be used as the base to perform further higher-level threat analysis. Based on this approach, every unknown activity or suspicious threat is labeled. The fundamental issues in sensor are accurate and timely performance to identify threats and the performance of a specific filter in blocking known and unknown threat [12].

2.4. Comparison between Traditional IPS and NGIPS

There are several common challenges in IPS such as deployment, management, technical, detection and response challenges. A summary of comparison between IPS and NGIPS is presented in Table 1.

A traditional IPS examines the traffic. It does not block the traffic beyond signature-based protection, while NGIPS goes way beyond signature-based security. NGIPS provides wide-range protection against vulnerabilities, deep packet inspection, real-time protection and able to control the behavior of the applications. Unlike traditional IPS, NGIPS has a huge number of features to tackle continuous changing pattern of the attacks.

2.5. Risk Assessment of IPS

Risk assessment and accuracy is a major concern of IPS systems. Figure 4 shows the relationship between accuracy, risk assessment and response of IPS. Generally, IPS triggers an alarm. An alarm can be either a false positive or a false negative. False positive alarm happens when the IPS report is positive that a harm action is malicious. This requires human intervention to analyse the event. False negative happens when the IPS does not detect and report actual malicious activity. The consequence of this can be disastrous; and signatures must be continually updated as new exploits and hacking techniques are found. The category of the accuracy rate is low, medium and high. When the attack types are known the accuracy should be high, normal and unknown attack accuracy is medium and low. The main goal of the next generation IPS systems is to increase the accuracy rate of normal and unknown attacks.

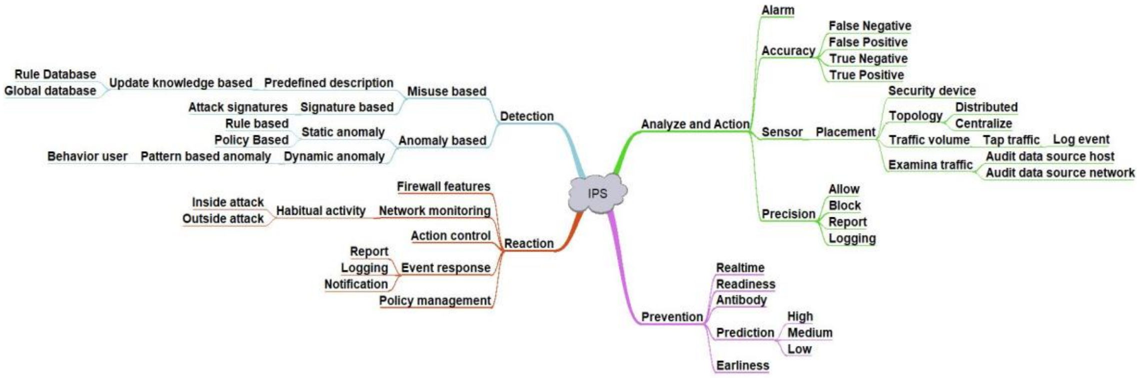

Fig. 3: Mapping Process of IPS

Table 1: Comparison between Traditional IPS and NGIPS

Features	Traditional IPS	NGIPS	Features	Traditional IPS	NGIPS
Core technology	Deep Packet Inspection	Deep Session Inspection	Network behavior analysis	No	Yes
Scalability and flexibility	Yes	Yes	User identity tracking	No	Yes
Intrusion detection and blocking	Yes	Yes	Networking mapping and host profile	No	Yes
Policy management	Yes	Yes	Content inspection	No	Yes
Have data loss prevention technology	No	Yes	Focus of attack	Server	Server and client
Able to detect and prevent unknown vulnerabilities	No	Yes	Advanced threat detection	Sandbox	Rules, Sandbox and Analytics
Application monitoring	No	Yes	Supports IPv6	No	Yes
Able to detect 0-day attack	No	Yes	Application protocols	No	Yes
Able to prevent from encrypted malware	No	Yes	Suitable for the cloud solutions	No	Yes
Malware	No	Yes	Mobile devices	No	Yes
Suitable for the virtualization technology	No	Yes	Third party integration supported	Yes	Yes
Have real time enforcement	No	Yes	False negative ratio	High	Low
Third party integration supported	Yes	Yes	Report and altering system	Yes	Yes

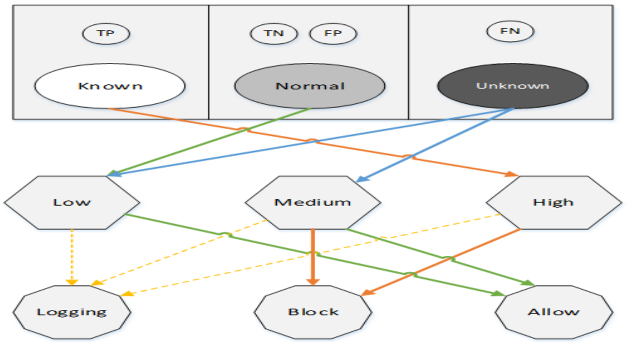

Fig. 4: Relationship between Accuracy, Risk Assessment and Response of IPS

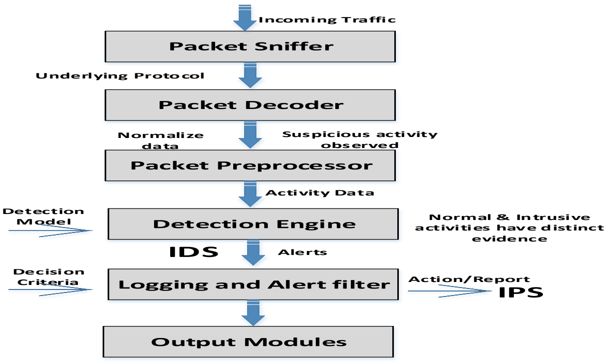

Fig. 5: Functions of Next Generation IPS in Network Security

2.6. Working Processes of NGIPS

Figure 5 shows the functions of Next Generation IPS in network security. In the NGIPS working process, packet decoder collects packets from different network interfaces and prepares it for the preprocessor. Preprocessors are being used to organize and modify packets. Detection engine analyzes all the packets passing through it to indicate whether any intrusion occurs by using certain predefined rules. Alert generation is used for creating the alert. The output modules display the results of intrusion detection examination.

3. Proposed Model for NGIPS

Based on the comprehensive review and analysis explained in Section 2, we propose an enhanced feature called as NBADS based on NGIPS features as displays in Figure 6. The acronym 'NBADS' stands for New Born Attack Detection System. It is a combination of snort signature and YARA signature. YARA signature is the improvement made for this NGIPS model. It is a new model, which consists of detection rules to detect and response to the incidents. The NBADS model will be simulated and tested in the future work.

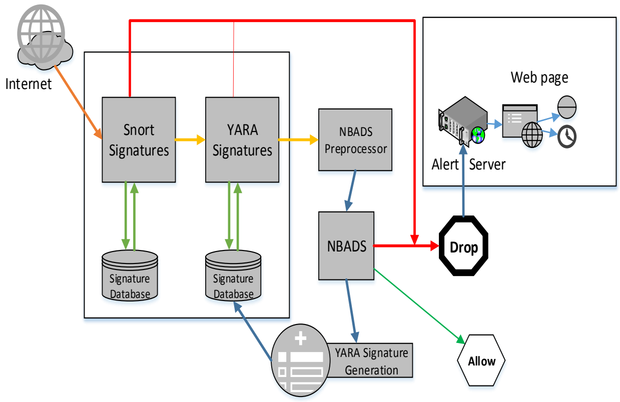

Fig. 6: Proposed Model of Next Generation IPS

4. Conclusion

There is a remarkable growth of technologies in computer network security, but still there is a huge lack of organizing resources for the prevention system. In this situation, Next Generation Intrusion Prevention System could provide the solution to the security world. In this paper, the limitations of traditional IPS systems were highlighted, the different aspects of traditional and next generation IPS were presented and a model of next generation IPS was proposed. The proposed working procedure and mapping processes of NGIPS can be used as the guidance and basis for future enhancement for NGIPS. The proposed model will consolidate signature and behavior-based detection, protocol and traffic anomaly detection, deep packet inspection and to detect recent threat intelligence attacks which will be tested in the future work.

Acknowledgement

The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM) for the support and facilities provided. This research paper is supported by grant: [PPP/USG-0116/FST/30/11716].

References

[1] Pirc, J. (2015). Next generation intrusion prevention is… So yesterday. White Paper. http://www.bricata.com.

[2] Bace, R. (1998). An introduction to intrusion detection and assessment. Infidel Inc.

[3] Woznick, D. (2014). Global information assurance certification paper. https://www.giac.org/paper/gcfw/441/giac-gcfw-assignment-pass/105451.

[4] Stiawan, D., Abdullah, A. H. & Idris, M. Y. (2011). Characterizing network intrusion prevention system. International Journal of Computer Application, 14(1), 11-18.

[5] Catherine, P. (2009). Network security using Cisco IOS IPS. Cisco Press.

[6] Ghorbani, A. A., Lu, W. & Tavallee, M. (2009). Network intrusion detection and prevention: Concepts and technique. Springer.

[7] Sekhar, R., Perumal, D. & Rani, S. (2015). Analysis of next generation intrusion prevention system using sensor fusion and fuzzy logic. International Journal of Scientific Research Engineering and Technology, 4(9), 936-938.

[8] Cisco. (2016). Cisco secure IPS - Excluding false positive alarms. https://www.cisco.com/c/en/us/support/docs/security/ips-4200-series-sensors/13876-f-pos.html#backinfo.

[9] Venter, H.S & Eloff, J.H.P. (2003). A taxonomy for information security technologies. Computers and Security, 22(4), 299-307.

[10] Zhang, S., Li, J., Chen, X. & Fan, L. (2008). Building network attack graph for alert causal correlation. Computers and Security, 27(5-6), 188-196.

[11] Kukielka, P., & Kotulski, Z. (2010). Adaptation of the neural network-based IDS to new attacks detection. https://arxiv.org/ftp/arxiv/papers/1009/1009.2406.pdf.

[12] Stiawan, D., Abdullah, A. H. & Idris, M. Y. (2010). Classification of habitual activities in behavior-based net-work detection. Journal of Computing, 2, 1-7.