A Comparative Performance Analysis of the Intrusion Detection Systems

Mohammed Saber[1](✉), Zineb Bougroun[1], Ilhame El Farissi[1], Sara Chadli[2], Mohamed Emharraf[1], Saida Belouali[3], Mohammed Ghaouth Belkasmi[1], and Ilham Slimani[1]

[1] Laboratory SmartICT, ENSAO, Université Mohammed Premier Oujda, Oujda, Morocco
m.saber@ump.ac.ma, bougroun.zineb@gmail.com, ilhame.elfarissi@gmail.com, m.emharraf@gmail.com, ghaouth@gmail.com, slimani.ilham@gmail.com

[2] Laboratory LSE, Sciences Faculty, Université Mohammed Premier Oujda, Oujda, Morocco
chad.saraa@gmail.com

[3] Laboratory LIDICOM, Université Mohammed Premier Oujda, Oujda, Morocco
saidabelouali@gmail.com

Abstract. In a comparative analysis, this paper investigates the performance of two open source intrusion detection systems (IDSs) namely SNORT and SURICATA for accurately detecting the malicious traffic on computer networks, an evaluation approach, based on a series of tests. These experiments consisted of a test bed which compared SNORT and SURICATA's reaction; consist in injecting various traffic loads, characterized by different transmission times, packet numbers, packet sizes and bandwidths, and then analyzing, for each situation, the processing performed on the packets. The study demonstrates that SURICATA would process a higher speed of network traffic than SNORT with lower packet drop rate but it consumed higher computational resources.

Keywords: Intrusion detection · SNORT · SURICATA · Performance comparison · Traffic network

1 Introduction

Recently, attacks made on computer networks have risen dramatically. These attacks are made at various layers in the TCP/IP protocol suite. The attackers act like normal users, generate data and hide their malicious activities under terabytes of data. The monitoring of the network traffic allows to detect malicious activities and perform analysis to differentiate the malicious and non malicious user activities to protect their networks. Detecting malicious activities require intrusion detection systems (IDS). It is critical that an IDS detection mechanism

A. El Moussati et al. (Eds.): SmartICT 2019, LNEE 684, pp. 192–200, 2020.
https://doi.org/10.1007/978-3-030-53187-4_23

is accurate enough to differentiate between legitimate and malicious traffic that enter and leave the network. The possible results of using an IDS are as follows: detected malicious traffic (real alarms), undetected malicious traffic, legitimate traffic that IDS detect as malicious (false alarms) and legitimate traffic that IDS detect as good.

Intrusion detection is difficult to be accomplished perfectly. With the volume of network traffic rapidly increasing and the number and complexity of network attacks increasing just as quickly, it becomes increasingly difficult for a signature-based intrusion-detection system to keep up with the current threats.

The evaluation performance of intrusion detection systems is a challenging task; it requires a thorough knowledge of techniques relating to different disciplines, especially intrusion detection, methods of attack, networks and systems, technical testing and evaluation.

Lately; more research is done on the evaluation of IDS, we cite some research in this area. In [1–4] the researchers evaluated the performance of three IDSs in an environment consisted of physical and virtual computers. The experiment results showed that SNORT could have a negative impact on network traffic more than the other two tested IDSs. In [5] a study demonstrated the lack of ability of SNORT IDS to process a number of packets at high speed and the packet drop rate was higher. The researchers introduced a parallel IDS technology to reduce the packet drop rate as a solution. The proposed approach significantly improved SNORT performance [6]. In papers [7,8] an evaluation of SNORT performance against DDoS. The experiments results show that SNORT packet handling could be improved by using better hardware configurations, but SNORT detection capability was not improved by using better hardware.

In [9], authors have tested and analysed the performance of SNORT and SURICATA. In [10], a comparison analysis of the performance of two open-source intrusion detection systems, SNORT and SURICATA is presented, by evaluating the speed, memory requirements, and accuracy of the detection engines in a variety of experiments. In [11] analysed and implemented the SNORT intrusion detection model in a campus network. In [12] presents a thorough comparison of the performance of SNORT and SURICATA. They examine the performance of both systems as they scale system resources. There are other works that looks at measuring the intrusion detection capability as in tweaking IDS performance as in [13], parallel design of IDS on many-core processors.

In [14], an approach for unifying rule based deep packet inspection and in [15], improving the accuracy of network intrusion detection systems. Whereas in [16], boosting throughput of SNORT NIDS under Linux. As in [17], evaluation studies of three IDS under various attacks and rule sets. In [18], evaluation based in classification of networks attacks [19]. The evaluation based in optimizes and analysis performance of an Intrusion Detection Systems, it is primordial to exploit uniquely the most important and crucial parameters of each features category KDD [20–22], etc.

This paper is structured as follows: 2^{nd} Section is devoted to the proposed approach for evaluating performance of the IDSs. Then a presentation and a discussion of the obtained results are shared in Sect. 3. Finally, 4^{th} Section which is dedicated to a conclusion and future works.

2 The Proposed Approach for Evaluating Performances IDS

The experiments consisted of a test bed which compared the performance of both IDSs. Experiment scenarios were designed to make observations and to take measurements. This study demonstrates rigorous, repeatable, quantitative performance comparison of both IDSs. The network traffic for the experiments was produced using network traffic generator. The default rule set of SNORT and SURICATA were used for the experiments.

2.1 Experiment Scenarios

- Scenario 1 (Consumed resources): The experiment compared the performance of both IDSs by measuring the percentage of CPU (Central Processing Unit), memory utilisation, with different traffic rates.
- Scenario 2 (Normal traffic accuracy measurements): The experiment was planned to determine the accuracy for both IDS ruleset inspected the network traffic to correctly classify the legitimate traffic network.
- Scenario 3 (Response to high-speed network traffic): The experiment compared the performance of both IDSs by measuring network packet drop rate, by the transmission of the packets (1460 bytes in size) at different transmission time frames (1, 4, 8 and 16 ms).

2.2 Experiment Network

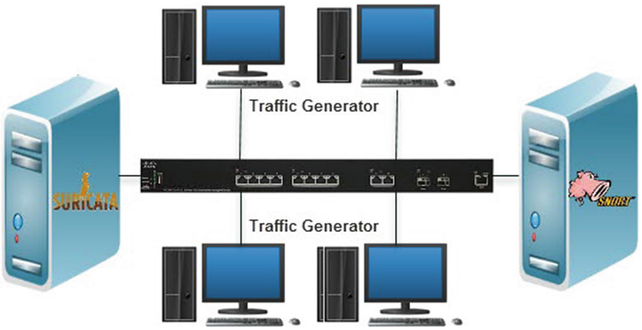

Fig. 1. Experiment network

To perform those tests, the SURICATA version 4.1.1 and the SNORT version 2.9.8.3 are selected. And for experimentations, the network shown in Fig. 1 is created. Four computers were used. Depending on the individual experiment requirements, network packets were produced at varying network speeds with network traffic generator tools. The four computers were connected via a switch CISCO SG350XG-2F10 using 10 Gbps Ethernet links. Each IDS was separately installed on identical computers with default performance parameters and rule set.

2.3 Performance Metrics

The metrics listed below in Table 1 are used to measure the detection accuracy of both IDSs.

Table 1. Description of performance metrics

Performance metrics	Description
False Positive Rate (FPR)	This is the likelihood that the IDS will trigger an alarm when there is no intrusion
False Negative Rate (FNR)	This is the likelihood that the IDS does not trigger an alarm when there is an intrusion
True Positive Rate (TPR)	This is the likelihood that IDS trigger an alarm when an intrusion is detected
Packets captured (PCA)	The number and percentage of packets received
Packets analysed (PAN)	The number and percentage of packets analysed from the total packets captured
Packets dropped (PDR)	The number and percentage of the packets dropped from the total packets captured

3 Experiment Scenarios Results and Evaluation

3.1 Experiment Scenario One : Consumed Resources

This first experimentation supervises the real-time performance of SNORT and SURICATA while processing at a different normal network speed from a network traffic generator. The rational behind the first experiment is to compare SNORT to SURICATA's performance. To achieve accurate results, the experiment scenario is tested with packets size of 1460 bytes. These packets were injected to both IDSs with a different network speed. The experiment consisted of a logical network diagram as shown in Fig. 1. Each IDS was separately installed on identical computers with default performance parameters and rule set. A number of tools were used to observe and record the measurements of CPU, memory, network utilisation and the packet drop rate. The following packets were injected as the background traffic ranging from a different network speed (100 Mbps, 250 Mbps, 500 Mbps, 750 Mbps, 1.0 Gpbs, 2.0 Gbps and 4.0 Gbps).

The collected performance data shows that SURICATA's CPU usage is greater than SNORT's as explained in Table 2. SURICATA's CPU utilisation is increased with different traffic rates, while SNORT's CPU utilisation is comparatively less using the same metrics.

Table 2. (%) CPU and Memory (GB) utilisation for SNORT and SURICATA for different traffic rates

Traffic rate	(%) CPU utilisation		Memory utilisation (GB)	
	SNORT	SURICATA	SNORT	SURICATA
100 Mbps	7	10	0.5	0.7
200 Mbps	12	17	0.7	1
250 Mbps	14	20	0.8	1.3
500 Mbps	23	30	1	1.7
750 Mbps	32	39	1.5	2.1
1.0 Gbps	39	48	1.8	2.7
2.0 Gbps	47	58	2.2	3.2
4.0 Gbps	55	68	2.4	3.5

The collected performance data shows that SURICATA's memory usage is greater than SNORT's as presented in Table 2. SNORT's memory usage was comparatively less. SURICATA's memory usage has to do more with the multithreaded architecture.

3.2 Experiment Scenario Tow: Normal Traffic Accuracy Measurements

This experiment is planned to determine how accurately SNORT's and SURICATA's rule set in order to inspect the network traffic and correctly classify the non malicious traffic. The metrics listed above in Table 1 are used to measure the detection accuracy of both IDSs.

Table 3. Normal traffic accuracy measurements

Normal traffic	SNORT			SURICATA		
	FPR	FNR	TPR	FPR	FNR	TPR
UDP	13%	0%	0%	22%	3%	0%
TCP	9%	0%	0%	33%	10%	0%
ICMP	2%	0%	0%	41%	29%	5%

The second experiment analyses the detection accuracy of SNORT and SURICATA while processing the legitimate network traffic. Both the IDSs were kept at the default setting. The accuracy test was performed using the legitimate network traffic generator which injected UDP, TCP and ICMP packets to both IDSs, the results are shown in Table 3. SURICATA's false positive rate (FPR) was higher when processing UDP, TCP and ICMP packets than SNORT's FPR. However, SNORT did not trigger true positive rate (TPR 0%) and false negative rate (FNR 0%) alarms. As compared to SURICATA, this triggered a 41% FNR and 5% TPR. Therefore, SNORT triggered less false positive alarms. While false negative alarms are observed in both IDSs, SNORT's detection accuracy is found to be superior to SURICATA in this scenario.

3.3 Experiment Scenario Three: IDSs Response to High-Speed Network Traffic

For this third scenario, the packets 1460 bytes in size (≅100000 TCP, and ≅100000 UDP, and ≅100000 ICMP) are sent at different transmission time frames (1 ms, 4 ms, 8 ms, and 16 ms) for the both systems. Figure 2 shows both IDSs output and obtained results.

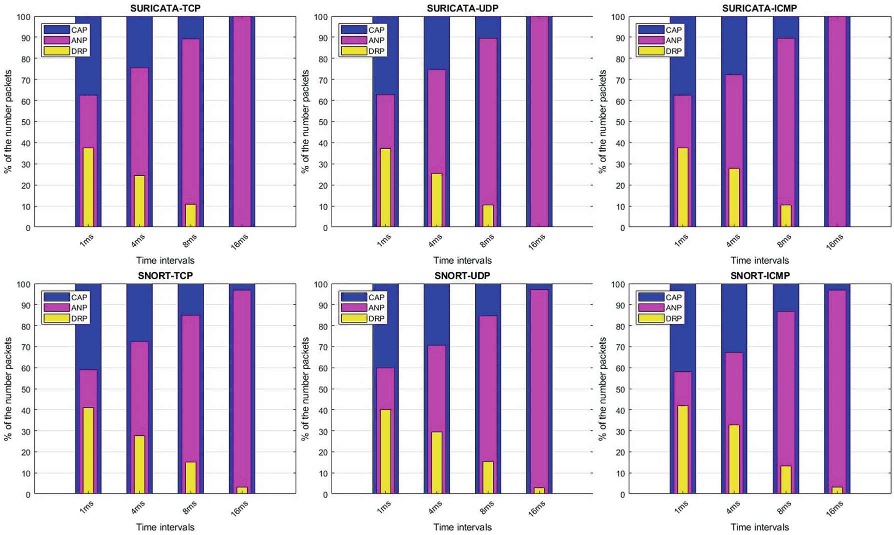

Fig. 2. IDSs response to high-speed network traffic

As demonstrated in the results shown in Fig. 2, all the sent packets reached their destinations. Both IDSs have analysed almost all packets in incoming traffic when packets are transmitted in 16 ms time frame. But when the speed of transmission is decreased, both IDSs start to drop packets. The collected performance data showed that SNORT's dropped packets is greater than that of SURICATA for the metrics (1 ms, 4 ms and 8 ms) as in Fig. 2.

In this experiment, it is noticed that for both IDSs; the analysis performance decreased as the speed of transmission is increased. Therfore, the components ability of analysis becomes weaker as the transmission speed is increased.

4 Conclusion

The main contribution of this study is the comparison of the intrusion detection performance of two open source IDSs, namely SNORT and SURICATA. Both are proved to be efficient and high performing IDS, although each one has its own strengths and weaknesses. The analysis of the experiment results shows that SNORT utilises less computational resources to process network traffic whereas SURICATA's utilisation was higher. Also, SURICATA processes a higher number of packets per second as compared to SNORT, and both IDSs have a high rate of false positives alarms. The obtained results demonstrate a number of signifficant limitations in the use of both IDS.

This work identifies specific and replicable bottlenecks in commonly used implementations IDS in high-speed networks. The obtained results can be taken as a benchmark to improve the performance of these systems in future research work.

References

1. Wang, X., Kordas, A., Hu, L., Gaedke, M., Smith, D.: Administrative evaluation of intrusion detection system. In: Proceedings of the 2nd Annual Conference on Research in Information Technology (RIIT 2013), pp. 47–52. ACM, New York (2013). https://doi.org/10.1145/2512209.2512216
2. Saber, M., Chadli, S., Emharraf, M., El Farissi, I.: Modeling and Implementation Approach to Evaluate the Intrusion Detection System. Springer (2015). https://doi.org/10.1007/978-3-319-26850-7_41
3. Shahbaz, M.B., Wang, X., Behnad, A., Samarabandu, J.: On efficiency enhancement of the correlation-based feature selection for intrusion detection systems. In: 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, pp. 1–7 (2016). https://doi.org/10.1109/IEMCON.2016.7746286
4. Saber, M., Belkasmi, M.G., Chadli, S., Emharraf, M.: Implementation and performance evaluation of network intrusion detection systems, pp. 484–495. Springer (2017). https://doi.org/10.1007/978-3-319-68179-5_42
5. Bulajoul, W., James, A., Pannu, M.: Network intrusion detection systems in high-speed traffic in computer networks. In: 2013 IEEE 10th International Conference on e-Business Engineering, Coventry, pp. 168–175 (2013). https://doi.org/10.1109/ICEBE.2013.26
6. Trabelsi, Z., Zeidan, S.: IDS performance enhancement technique based on dynamic traffic awareness histograms. In: 2014 IEEE International Conference on Communications (ICC), Sydney, NSW 2014, pp. 975–980 (2014). https://doi.org/10.1109/ICC.2014.6883446

7. Saboor, A., Akhlaq, M., Aslam, B.: Experimental evaluation of SNORT against DDoS attacks under different hardware configurations. In: 2013 2nd National Conference on Information Assurance (NCIA), Rawalpindi, pp. 31–37 (2013). https://doi.org/10.1109/NCIA.2013.6725321
8. Saber, M., Emharref, M., Bouchentouf, T., Benazzi, A.: Platform based on an embedded system to evaluate the intrusion detection system. IEEE Xplore Digital Libr. 894–899 (2012). https://doi.org/10.1109/ICMCS.2012.6320253
9. Alhomoud, A., Munir, R., Disso, J.P., Awan, I., Al-Dhelaan, A.: Performance evaluation study of intrusion detection systems. Procedia Comput. Sci. **5**, 173–180 (2011). https://doi.org/10.1016/j.procs.2011.07.024, ISSN 1877-0509
10. Karim, I., Vien, Q.-T., Le, T.A., Mapp, G.: A comparative experimental design and performance analysis of SNORT-based Intrusion Detection System in practical computer networks. Computers **6**(1), 1–15 (2017). https://doi.org/10.3390/computers6010006, ISSN 2073-431X
11. Huang, C., Xiong, J., Peng, Z.: Applied research on SNORT intrusion detection model in the campus network. In: 2012 IEEE Symposium on Robotics and Applications (ISRA), Kuala Lumpur, pp. 596–599 (2012). https://doi.org/10.1109/ISRA.2012.6219259
12. White, J.S., Fitzsimmons, T., Matthews, J.N.: Quantitative analysis of intrusion detection systems: SNORT and SURICATA. In: Proceedings of SPIE - (2013) The International Society for Optical Engineering, vol. 8757. https://doi.org/10.1117/12.2015616
13. Hafeez, K., Masood, M., Malik, O., Anwar, Z.: LASSP: a logic analyzer for tweaking SNORT security and performance. In: 2010 6th International Conference on Emerging Technologies (ICET), Islamabad, pp. 240–245 (2010). https://doi.org/10.1109/ICET.2010.5638483
14. Jiang, H., Zhang, G., Xie, G., Salamatian, K., Mathy, L.: Scalable high-performance parallel design for network intrusion detection systems on many-core processors. In: Proceedings of the Ninth ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2013), Piscataway, NJ, USA, pp. 137–146. IEEE Press (2013)
15. Munoz, A., Sezer, S., Burns, D., Douglas, G.: An approach for unifying rule based deep packet inspection. In: 2011 IEEE International Conference on Communications (ICC), Kyoto, pp. 1–5 (2011). https://doi.org/10.1109/icc.2011.5963095
16. Papadogiannakis, A., Polychronakis, M., Markatos, E.P.: Improving the accuracy of network intrusion detection systems under load using selective packet discarding. In: Proceedings of the Third European Workshop on System Security (EUROSEC 2010), pp. 15–21. ACM, New York (2010). https://doi.org/10.1145/1752046.1752049
17. Salah, K., Qahtan, A.: Boosting throughput of SNORT NIDS under Linux. In: 2008 International Conference on Innovations in Information Technology, Al Ain, pp. 643–647 (2008). https://doi.org/10.1109/INNOVATIONS.2008.4781733
18. Thongkanchorn, K., Ngamsuriyaroj, S., Visoottiviseth, V.: Evaluation studies of three intrusion detection systems under various attacks and rule sets. In: 2013 IEEE International Conference of IEEE Region 10 (TENCON 2013), Xi'an, pp. 1–4 (2013). https://doi.org/10.1109/TENCON.2013.6718975
19. Saber, M., Bouchentouf, T., Benazzi, A., Azizi, M.: Amelioration of attack classifications for evaluating and testing intrusion detection system. J. Comput. Sci. **6**(N7), 716–722 (2010). https://doi.org/10.3844/jcssp.2010.716.722

20. El Farissi, I., Saber, M., Chadli, S., Emharraf, M., Belkasmi, M.G.: The analysis performance of an Intrusion detection systems based on neural network. IEEE Xplore Digital Libr. 145–151 (2017). https://doi.org/10.1109/CIST.2016.7805032
21. El Farissi, I., Chadli, S., Emharraf, M., Saber, M.: The analysis of KDD-parameters to develop an intrusion detection system based on neural network, pp. 491–503. Springer (2017). https://doi.org/10.1007/978-981-10-1627-1_39
22. Saber, M., El Farissi, I., Chadli, S., Emharraf, M., Belkasmi, M.G.: Performance analysis of an intrusion detection systems based of artificial neural network. Springer (2017). https://doi.org/10.1007/978-3-319-46568-5_52