Performance Analysis of IDS Snort and IDS Suricata with Many-Core Processor in Virtual Machines Against Dos/DDoS Attacks

Dede Fadhilah
Electrical Engineering Department
Universitas Mercu Buana
Jakarta, Indonesia
defadhilah@gmail.com

Marza Ihsan Marzuki
Electrical Engineering Department
Universitas Mercu Buana
Jakarta, Indonesia
marza.ihsan@mercubuana.ac.id

***Abstract*— The rapid development of technology makes it possible for a physical machine to be converted into a virtual machine, which can operate multiple operating systems that are running simultaneously and connected to the internet. DoS/DDoS attacks are cyber-attacks that can threaten the telecommunications sector because these attacks cause services to be disrupted and be difficult to access. There are several software tools for monitoring abnormal activities on the network, such as IDS Snort and IDS Suricata. From previous studies, IDS Suricata is superior to IDS Snort version 2 because IDS Suricata already supports multi-threading, while IDS Snort version 2 still only supports single-threading. This paper aims to conduct tests on IDS Snort version 3.0 which already supports multi-threading and IDS Suricata. This research was carried out on a virtual machine with 1 core, 2 core, and 4 core processor settings for CPU, memory, and capture packet attacks on IDS Snort version 3.0 and IDS Suricata. The attack scenario is divided into 2 parts: DoS attack scenario using 1 physical computer, and DDoS attack scenario using 5 physical computers. Based on overall testing, the results are: In general, IDS Snort version 3.0 is better than IDS Suricata. This is based on the results when using a maximum of 4 core processor, in which IDS Snort version 3.0 CPU usage is stable at 55% - 58%, a maximum memory of 3,000 MB, can detect DoS attacks with 27,034,751 packets, and DDoS attacks with 36,919,395 packets. Meanwhile, different results were obtained by IDS Suricata, in which CPU usage is better compared to IDS Snort version 3.0 with only 10% - 40% usage, and a maximum memory of 1,800 MB. However, the capabilities of detecting DoS attacks are smaller with 3,671,305 packets, and DDoS attacks with a total of 7,619,317 packets on a TCP Flood attack test.**

Keywords—IDS, intrusion detection system, snort, suricata, DoS, DDoS

I. INTRODUCTION

In the current era of technological development, virtual machines can be relied upon to operate multiple operating systems using only one physical machine. Users can make a virtual machine as a file-sharing server that can be connected to the internet. However the downside is that, this can cause a virtual machine to be vulnerable to cyber-attacks, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which can attack and dissipate resources owned by the server or machine to cause the services on the server becoming unavailable.

The author of [1] said in his publication with data obtained from the UCSD Network Telescope, revealed that in Denial of Service (DoS) attacks from March 2015 - February 2017, there was 20 million Denial of Service (DoS) attacks targeting 2.2 million IP Addresses, in which there were more than a third of them are thought to be active IP Addresses.

Other data reports [2] stated that in Q1 2018 there were 2.8 million DDoS attacks, which increased by 39% in Q1 2019 to around 3.8 million DDoS attacks. Until Q1 2019, DDoS attacks mainly targeted 4 industrial sectors such as: Cable Telecommunications, Satellite, Hosting, Wireless Operators, and related services. [2]

In preventing and protecting from DoS / DDoS attacks, there are open package sources that are acknowledged by IT, particularly intrusion detection system and intrusion prevention system (IDS / IPS). One example of these systems is IDS Snort and IDS Suricata which can monitor and protect networks or servers from cyber-attacks, such as DoS / DDoS attacks.

From previous research, we know that IDS Snort version 2 can only run on single-threading architecture while IDS / IPS Suricata can run on multi-threading architecture [3], which are how many cores on a computer. This means IDS Snort can only use single core or single thread.

In a previous study in 2018 [4], the authors made a comparison between IDS Snort version 2 with IDS Suricata, in which the authors explicitly stated that the performance of IDS Suricata outperformed IDS Snort version 2.

A. *Contribution of the Research*

In a previous study [4] it was found that IDS Snort version 2 does not support multi-threading and that performance of IDS Suricata is better than IDS Snort. Furthermore, we know that IDS Snort version 3 already supports multi-threading. Specific discussion regarding the role of multi-threading in both IDS for utilizing processor cores in detecting network attacks needs to be discussed to determine the performance of multi-threading performance. This includes analysis regarding the differences in the character of multi-threading performance between the two IDSs in detecting attacks, identifying DoS / DDoS attacks, and analyzing the packet drop generated by both of these IDS is necessary to assist organizations in selecting an intrusion detection system that is cheap and reliable.

978-1-7281-7450-1/20/$31.00 ©2020 IEEE

II. Related Work

A recent research conducted on IDS Snort 3.0 and IDS Suricata 4.1 experimented and examining on how much packet drop will occurs on high-speed networks with throughput of 10 Gb/s to 100 Gb/s with 1500 bytes packet size using Iperf and Pytbull for 1800 seconds [6]. This test is performed on physical machines with 12 core processors and 196 GB of memory, with both IDS using the default rules. The results of the study showed IDS Snort and IDS Suricata had a limitation of up to 10 Gb/s in processing packet traffic, and the experimental results showed that the IDS packet drop results were only 0.01%. The research was continued by replaying packet traffic from the Trex tool and processing 33,000 flow (about 2 Gb/s of network traffic) per second. The result is IDS Snort experiencing a packet drop of up to 99.9%, and IDS Suricata 68%.

Analysis related to IDS Snort in detecting DDoS attacks was conducted in the cloud computing environment where this research runs the attacker and IDS Snort on GNS3, where GNS3 is run on VMware [7]. The experiment used 2 attackers, and the tools used were LOIC tools with attack mode that is TCP Syn Flood. The authors also make rules with actions that are "drop" to detect DDoS attacks. The results of this study are IDS Snort can detect and reset connections in DDoS attacks and CPU increases up to 65%.

The dataset IDEVAL (Intrusion Detection Evaluation) is used to identify various attacks on computer networks by using samples of network traffic and audit logs that are used to evaluate intrusion detection systems on IDS Snort [8]. The author measures the probability of detection and the possibility of false alarms for each system tested. The result is IDS Snort can detect known attack patterns using base signatures, so that unknown attacks will be detected via anomaly-based IDS Snort. IDS Snort is used to detect attacks likewise as preventative measures, and IDS Snort must be updated frequently to get used to the latest patterns of attacks and threats.

Research [9] conducted an experiment related to a comparison between IDS Suricata 1.0.2 performance with IDS Snort 2.9.0.4 on Windows and Linux CentOS operating systems using bad traffic attacks, fragmented packets, brute force, evasion techniques, denial of services, and test rules. In that research, it is known that IDS Snort and Suricata use more resources in the Linux operating system than Windows, but the Windows operating system experiences a lot of packet drops which renders both of these IDS inappropriate for use on Windows operating systems. Based on research experiments, researchers stated that IDS Suricata has better performance than IDS Snort.

To maximize the performance of the network intrusion detection system (NIDS), the authors conducted an experimental test using NIDS Snort 2.9.2.1 and NIDS Suricata to be tested on servers with Intel CPU specifications. E5-2690 TILE-Gx72 CPUs with 32GB RAM, where the processor has 72 processor cores [10]. The author sends HTTP packets using a packet generator to the server for up to 79 Gbps, and this resulted in an additional increase in performance by an average of 32%.

A. *Literature Review*

The following section is an update on the IDS Snort 3.0 architecture which can use multi-threading.

1) IDS Snort Architecture

IDS Snort has five main components: packet capture, packet decoder, preprocessor, detection engine, and output. First, IDS Snort will collect all network packets using libpcap, analyze packet traffic originating from the ethernet card, and then forwarded it by using the packet decoder. This component will process each packet in sequence and decode part of the data link protocol (Ethernet, token ring, 802.11), network protocol (IP, ICMP), and then transport protocol (TCP, UDP). The results of the process are sent to the preprocessor. Next, the preprocessor will be analyzed to perform TCP reassembly, reassembling packet fragments, and tracking TCP and UDP sessions. If the preprocessor discovers an anomaly packet, the preprocessor will stop the packet process before the detection engine processes the packet. In IDS Snort 3.0, the more processor cores used, the more packet processing threads can be used. After all of the processes are run, IDS Snort will log and trigger alerts based on actions in the rules. The output results can be in the form of statistical reports, log in the form of text, CSV, XML, or database [6]

2) IDS Suricata Architecture

IDS Suricata architecture has similarities with IDS Snort but has a difference where IDS Suricata does not use preprocessor components in its architecture but uses packet decoder and detection engine [11]. IDS Suricata uses library af_packet to improve performance in capturing network packets and analyzing them from NIC cards. Then the packet is forwarded to the packet decoder [12]. In the packet decoder module, every packet starting from the data link protocol to the transport protocol will be processed and changed to a Suricata supporting data structure. Then the packet is forwarded to the detection engine. In this process, the detection engine is governed by rules. Rules IDS Suricata supports layer 3, layer 4, and layer 7. Rules contain signatures that match internal packet representations. This matching process is divided into several detection engine modules where all packets and matching rules are performed. If there is a dangerous packet that matches the rules, it will be forwarded to output [11].

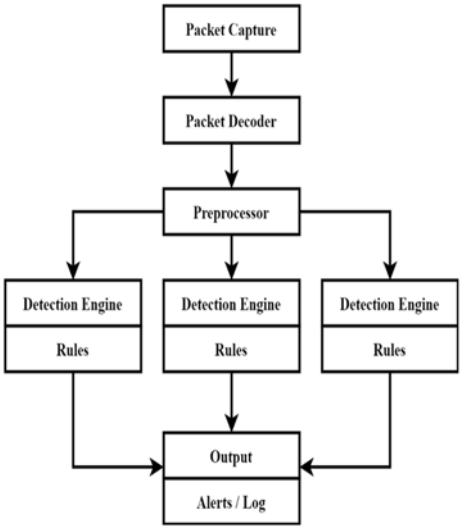

Fig. 1. IDS snort 3.0 architecture [6]

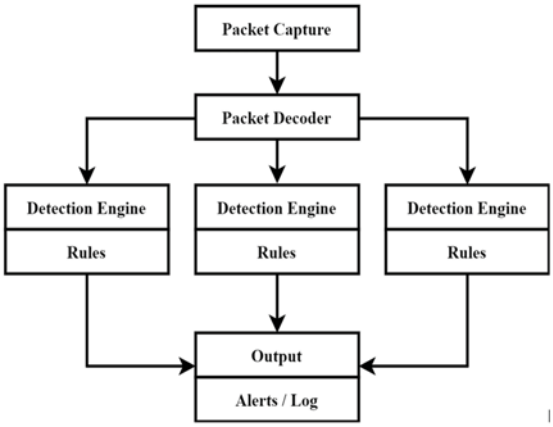

Fig. 2. IDS suricata architecture [12]

III. METHODS

Topology research design schemes from this research can be seen in Fig. 3. In this study, we made a trial design using 5 units of computers and 3 virtual machines. We create 1 VM web server as the targeted attack, 1 VM IDS Snort, and 1 VM IDS Suricata as monitoring traffic DoS/ DDoS attacks. We use IDS Snort version 3.0.0-263, and IDS Suricata version 5.0.3.

In running virtualization, we use laptops with Intel Core i5-5200U CPU @ 2.20GHz (4 CPUs) with 8 GB RAM with Windows operating system to run a virtual machine (VM) Web Server, VM IDS Snort and VM IDS Suricata.

In this experiment, to avoid interruption in the collection of analytical data, we tested the performance of IDS Snort and IDS Suricata by running both IDS alternately with the VM Web Server as the target of the attack.

A. *Scenario DoS Attacks*

For scenario testing DoS attacks, we use 1 computer as an attacker and run LOIC tools using the TCP Syn Flood and UDP Flood attacks with 5 minutes to attack the target.

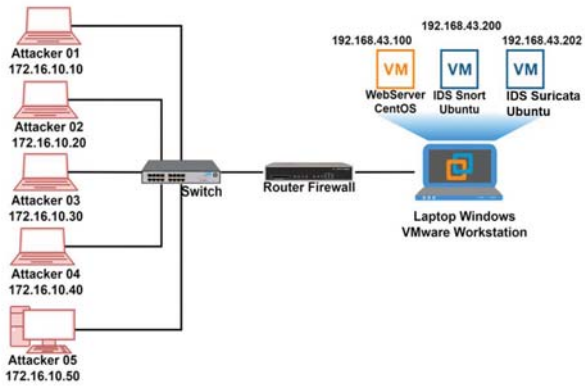

Fig. 3. Design topology

B. *Scenario DDoS Attacks*

For scenario testing DDoS attacks, we use 5 computer attackers. The attack test is carried out for 5 minutes, according to which [13] DDoS attacks last less than 15 minutes, according to [14] to avoid attacks being detected, the normal attack time is 10 minutes, and according to [15] [16] states that DDoS attacks usually shorter duration of about 5 minutes or less.

To improve detection accuracy, we create local rules to detect DoS and DDoS attacks.

1) "alert tcp any any -> 192.168.43.100 80 (msg: "TCP Syn Flood DoS Attack Detected!"; sid:10000001;)"
2) alert udp any any -> 192.168.43.100 80 (msg: "UDP Flood DoS Attack Detected!; sid:10000002;)"

Based on these rules, IDS Snort will detect attacks with the destination IP address of the VM Web Server (192.168.43.100 port 80) with attacks coming from anywhere, with alerts tailored to the type of attack. The Rules used for DoS and DDOS are similar, the difference is only in the message alert.

In this experiment, the rules used in IDS Snort and IDS Suricata are the same. According to [11] rules on IDS Snort can be used and compatible on IDS Suricata.

For testing using different processor cores, VMware Workstation has a feature to change the use of processor cores. This experiment uses 1 core, 2 core, and 4 core processor settings in the VM IDS Snort and VM IDS Suricata.

In running detection mode on both IDS, the experiment on IDS Snort uses command (1), and IDS Suricata uses command (2) as follows:

1) *timeout 300 snort -c /usr/local/etc/snort/snort.lua –R /usr/local/etc/snort/rules/local.rules \ -i eth0 -A alert_fast -s 65535 -k none --max-packet-threads*
2) *timeout 300 suricata -c /etc/suricata/suricata.yaml -i eth0 --runmode workers*

In running detection mode on IDS Snort, we use automatic commands for testing the duration of five minutes, and use local rules with the addition of the command "--max-packet-threads" where IDS Snort 3.0 can run threads to process packet traffic from network interfaces with an adjusted number of threads with a number of processor cores up to 8 threads [17].

In IDS Suricata, we use the command "--runmode workers" which means in this mode, processing threads will process all packets equally. According to Official Suricata, runmode workers is the best mode.

Fig. 4. Core processor settings

In this research, the best detect mode for IDS Snort and IDS Suricata is used to detect attacks. This research aims to determine the character of multi-threading performance in using and utilizing the core processor on both IDS in detecting DoS / DDoS attacks.

IV. Results

The results of this experiment display comparative data on CPU, Memory, and Packet resources that have been detected by IDS Snort and IDS Suricata for five minutes.

A. *Comparison Performance of CPU and Memory IDS Snort and IDS Suricata*

In table I is the result of DoS attack testing with testing using 1 core, 2 cores, and 4 processor cores. From this data, when using 1 core processor, the use of CPU IDS Snort is very high around 98% - 99%, but when using a maximum of 4 processor cores, CPU usage is more stable at 58%. In memory usage, there is an increase in memory up to 600 MB when using a maximum of 4 core processors

In IDS Suricata, the consumption of IDS CPU usage is more stable and lower than IDS Snort with CPU usage around 10% to 30% when using a maximum of 4 processor cores. In memory usage, IDS Suricata looks stable when it detects a DoS attack which only increases about 100MB.

In table II, from the results of the DDoS attack experiment, we obtain data that CPU and Memory usage on IDS Suricata is lower than IDS Snort when detecting DDoS attacks.

B. *Comparison of Captured Packet of DoS and DDoS Attacks*

In fig 5, and 6 are the results of experiments and comparison of DoS and DDoS attacks. Based on data, we knew that the command usage "--max-packet-threads" has been proven to improve the performance of IDS Snort 3.0 packet threading in detecting attacks, which makes the number of attacks captured successfully increase directly proportional to the number of processor cores used.

Table I. Comparison of CPU and Memory (DoS Attacks)

IDS	DoS Attack	CPU 1 Core		CPU 2 Core		CPU 4 Core	
		CPU (%)	RAM (MB)	CPU (%)	RAM (MB)	CPU (%)	RAM (MB)
Snort	No Attack	5	1700	5	1700	5	1700
	TCP Flood	98	2000	90	2200	58	2300
	UDP Flood	99	1900	96	2000	58	1900
Suricata	No Attack	5	1600	5	1600	5	1700
	TCP Flood	25	1700	20	1700	30	1800
	UDP Flood	40	1700	20	1700	10	1800

Table II. Comparison of CPU and Memory (DDoS Attacks)

IDS	DDoS Attack	CPU 1 Core		CPU 2 Core		CPU 4 Core	
		CPU (%)	RAM (MB)	CPU (%)	RAM (MB)	CPU (%)	RAM (MB)
Snort	No Attack	5	1700	5	1700	5	1700
	TCP Flood	98	2600	96	3100	58	3000
	UDP Flood	92	1800	85	1900	55	2000
Suricata	No Attack	5	1600	5	1600	5	1700
	TCP Flood	80	1700	20	1700	17	1800
	UDP Flood	40	1700	35	1700	17	1800

In the attempted DoS and DDoS attacks, the multi-threading performance on IDS Suricata did not show good performance. When the use of processor cores increases, it does not prove an increase in performance in capturing packet attacks. We found a research article [18] which states that multi-threading on IDS Suricata does not reflect better performance when using more CPU cores.

From these data, it can be seen in DoS attack testing, the type of attack most captured is TCP Syn Flood DoS attack. However, when testing DDoS attacks, the most captured type of attack is DDoS UDP Flood

In tables III and IV, it is the percentage of packet drop obtained when attempting a DoS and DDoS attack on IDS Snort and IDS Suricata.

In the experiment DoS and DDoS attacks, with maximum use of 4 processor cores, IDS Snort has a very high percentage drop with a percentage of DoS 88.04% (TCP Syn Flood), 80.69% (UDP Flood), and DDoS 95.98% (TCP Syn Flood), 99.43% (UDP Flood). Different results obtained IDS Suricata with a packet drop of 0.01% DoS (TCP Syn Flood and UDP Flood)

After obtaining statistical data packets from DoS and DDoS attacks, we tried to look for packets per second and packet size for DoS and DDoS attacks.

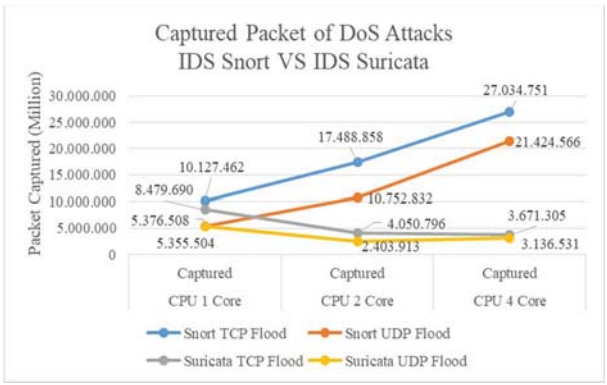

Fig. 5. Comparison of captured packet of DoS attacks

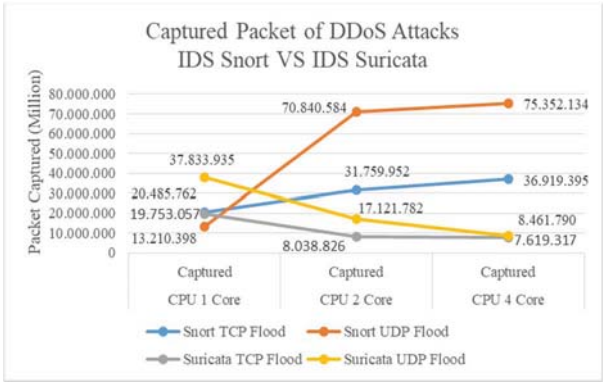

Fig. 6. Comparison ofcCaptured packet of DDoS attacks

In this experiment, we monitored both of these IDS and obtained data that the throughput of attacks generated by the LOIC tools was 16 Mbps for DoS TCP Syn Flood, 8 Mbps for DoS UDP Flood. In the DDoS TCP Syn Flood attack, throughput reaches 320 Mbps, and DDoS UDP Flood reaches 100 Mbps.

According to RFC 7141 [19], IETF defines the minimum packet size is 60 bytes, and the maximum packet size is 1500 bytes. Based on calculations [20], if known throughput and packet per second, then to calculate packet size, are as follows:

1) Calculating packet per second :

   10.127.462 packet / 300 second = 33.758 packet capture per second (pps)

2) Calculating packet size :

   16 Mbps = (16.000.000 bits/s) / (8 bits/byte) = 2.000.000 bytes/s

   Packet Size = (2.000.000 bytes/s) / 33.758 pps = 59 Bytes/packet

From table V, it appears that in a DoS attack, the packet size sent by the attacker and captured by the IDS Snort is smaller than the standard set by the IETF.

From table V and table VI, data shows that the LOIC attack tool tries to send attack packets that can make the target web server resources full. From these data, we know that IDS Snort can capture more packets per second than IDS Suricata.

In a DoS attack, the average packet size captured by IDS Snort has a packet size of less than 60 bytes, this indicates that the DDoS LOIC tool can modify the packet size below the standard packet size to establish a connection to the target, and to attack with packets that are already modified.

According to [21] in his dissertation, the TCP DoS attack has an abnormal packet size of less than 64 bytes in order to exploit TCP protocol design flaws and avoid detection, and according to [22] a packet size of fewer than 60 bytes is a packet that does not have data payload.

TABLE III. COMPARISON OF PACKET DROP DOS ATTACKS

IDS	DoS Attack	CPU 1 Core	CPU 2 Core	CPU 4 Core
		Dropped (%)	Dropped (%)	Dropped (%)
Snort	TCP Flood	92,32%	84,55%	88,04%
	UDP Flood	83,14%	74,59%	80,69%
Suricata	TCP Flood	0,02%	0,10%	0,01%
	UDP Flood	0,21%	0,00%	0,01%

TABLE IV. COMPARISON OF PACKET DROP DDOS ATTACKS

IDS	DDoS Attack	CPU 1 Core	CPU 2 Core	CPU 4 Core
		Dropped (%)	Dropped (%)	Dropped (%)
Snort	TCP Flood	97,98%	95,73%	95,98%
	UDP Flood	95,96%	98,36%	99,43%
Suricata	TCP Flood	0,36%	0,38%	0,15%
	UDP Flood	1,21%	0,98%	7,37%

TABLE V. PACKET CAPTURE PER SECOND AND PACKET SIZE DOS

IDS	DoS Attack	1 Core		2 Core		4 Core	
		Packet Capture (1s)	Packet Size (Bytes)	Packet Capture (1s)	Packet Size (Bytes)	Packet Capture (1s)	Packet Size (Bytes)
Snort	TCP Flood	33.758	59	58.296	34	90.116	22
	UDP Flood	17.922	56	35.843	28	71.415	14
Suricata	TCP Flood	28.266	71	13.503	148	12.238	163
	UDP Flood	17.852	56	8.013	125	10.455	96

TABLE VI. PACKET CAPTURE PER SECOND AND PACKET SIZE DDOS

IDS	DDoS Attack	1 Core		2 Core		4 Core	
		Packet Capture (1s)	Packet Size (Bytes)	Packet Capture (1s)	Packet Size (Bytes)	Packet Capture (1s)	Packet Size (Bytes)
Snort	TCP Flood	68.286	586	105.867	378	123.065	325
	UDP Flood	44.035	284	236.135	53	251.174	50
Suricata	TCP Flood	65.844	608	26.796	1.493	25.398	1.575
	UDP Flood	126.113	99	57.073	219	28.206	443

Based on [23], the author states that attacks with high packet size (high rate, around 1500 bytes), these attacks can be easily detected, but on attacks with low packet size (low rate) can be used to exploit vulnerabilities in the mechanism protocol TCP, where the attacker sends attacks regularly in a short period of time repeatedly or continuously sending packet attacks with a low packet size to avoid attacks being detected. The author [23] uses a dataset from CAIDA and classifies a low packet rate into 2 parts, namely a packet size of fewer than 60 bytes, and a packet size of about 1400 bytes for DDoS, and classifies a low packet rate = 1000 packets per second, and high packet rate = 10,000 - 100,000 packets per second.

From the research review [23], we tried to classify the data obtained from this study with the classification conducted by [23]. After calculating the packet size, we found that the packet size detected by IDS Snort ranges from 22 bytes - 59 bytes (TCP Syn Flood), and 14 bytes - 56 bytes (UDP Flood). We conclude that DoS attacks generated by DDoS LOIC tools are Low Rate DoS Attack, but the packet size obtained by IDS Suricata ranges from 71 bytes - 163 bytes (TCP Syn Flood) and 56 bytes - 96 bytes (UDP Flood), so it can be said that the packet size obtained by IDS Suricata is not a packet size categorized as Low-Rate.

In DDoS attacks, IDS Snort can capture attack packets up to 123,064 pps (TCP Syn Flood), and 251,174 pps (UDP Flood), can be categorized as high packet rate, and in IDS Suricata can capture attack packets up to 25,398 pps (TCP Syn Flood) Flood), and 28,206 pps (UDP Flood), can be categorized as high packet rate.

Based on experiment, packet drop in IDS Snort could reach 99.43%, and the IDS Suricata packet drop was 7.37%. After we match the results of packet size calculations, we conclude that Snort IDS can detect Low Rate DoS attacks, which in Low Rate DoS attacks are used to exploit the design of the TCP protocol and avoid detection systems. IDS Snort uses a preprocessor module to help detect anomaly packets before being forwarded to engine detection so that when a packet is detected as an abnormal packet, IDS Snort will drop the packet before it is forwarded to the engine detection.

Based on research [11], the IDS Suricata architecture does not have a preprocessor module. This makes it difficult for

IDS Suricata to detect packet anomalies with the type of Low Rate DoS Attack used by LOIC tools, where this type of attack is able to exploit a vulnerability in the TCP design mechanism that causes IDS Suricata to classify it as a normal packet, which causes a small packet drop.

V. Conclusions and Future Work

The results of DoS and DDoS attacks on IDS Snort and IDS Suricata, it is found that the CPU and Memory performance of IDS Suricata in detecting attacks is quite stable and better than that of IDS Snort, but the performance of IDS Suricata when detecting packet attacks does not show an increase in the number of detection attacks. when the number of cores used increases. In IDS Snort 3.0 when using a maximum of 4 processor cores, CPU usage is stable at 55% to 58% and there is a significant increase in detecting DoS / DDoS attacks as the number of processor cores increases. From these data, it can be concluded that the multi-threading performance on IDS Snort 3.0 is better than IDS Suricata.

For further research, we highly recommend to use QoS to control incoming and detected packet traffic properly by those two IDS, and another method is needed to make packet threading on IDS Suricata better.

References

[1] M. Jonker, A. King, J. Krupp, C. Rossow, A. Sperotto, & A. Dainotti, "Millions of targets under attack: A macroscopic characterization of the DoS ecosystem," Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC, Part F131937, 2017, 100–113.

[2] Netscout, "Netscout Threat Report 1H 2019." [Online]. Available: https://www.netscout.com/threatreport.

[3] S. Shah, & B. Issac, "Performance comparison of intrusion detection systems and application of machine learning to snort system," Future Generation Computer Systems, 80, 157-170, 2018

[4] E. Ficke, K. M. Schweitzer, R. M. Bateman, & S. Xu, "Characterizing the effectiveness of network-based intrusion detection systems," MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM).

[5] Snort, "Snort 3 User Manual." [Online]. Available: https://www.snort.org/downloads/snortplus/snort_manual.pdf

[6] Q. Hu, S.-Y. Yu, & M. R. Asghar, "Analysing performance issues of open-source intrusion detection systems in high-speed networks," Journal of Information Security and Applications, 51, 2020, 102426.

[7] Z. Hassan, Shahzeb, R. Odarchenko, S. Gnatyuk, A. Zaman, & M. Shah, "Detection of distributed denial of service attacks using snort rules in cloud computing & remote control systems," 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC).

[8] A. Garg, & P. Maheshwari, "Performance analysis of snort-based intrusion detection system," ICACCS 2016 - 3rd International Conference on Advanced Computing and Communication Systems: Bringing to the Table, Futuristic Technologies from Around the Globe.

[9] B. Brumen, & J. Legvart, "Performance analysis of two open source intrusion detection systems," 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2016 - Proceedings, 1387–1392.

[10] J. Nam, M. Jamshed, B. Choi, D. Han, & K. S. Park, "Haetae: Scaling the performance of network intrusion detection with many-core processors," Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9404, 2015, 89–110.

[11] I. Ghafir, V. Prenosil, J. Svoboda, & M. Hammoudeh, "A survey on network security monitoring systems," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW).

[12] OISF, "Suricata User Guide Release 5.0.3." [Online]. Available: https://suricata.readthedocs.io/_/downloads/en/suricata-5.0.3/pdf/.

[13] Fortinet, "FortiDDoS Data Sheet." [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiddos.pdf.

[14] L. Zhou, M. Liao, C. Yuan, & H. Zhang, "Low-rate DDoS attack detection using expectation of packet size," Security and Communication Networks, 2017, 1–14.

[15] B. Nagy, P. Orosz, & P. Varga, "Low-reaction time FPGA-based DDoS detector," NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium.

[16] GTT, "How To Handle A Ransom-Driven DDoS Attack." [Online]. Available: https://www.gtt.net/media/1444/how-to-handle-a-ransom-driven-ddos-attack-ebook.pdf.

[17] Snort, "Snort 3 Multiple Packet Processing Threads." [Online]. Available: https://www.snort.org/documents/snort-3-multiple-packet-threads -processing.

[18] X. Bu, "Performance Characterization of Suricata's Thread Models" [Online]. Available: https://xbu.me/article/performance-characterization-of-suricata-thread-models/

[19] IETF, "Byte and Packet Congestion Notification." [Online]. Available from: https://tools.ietf.org/html/rfc7141.

[20] Juniper, "How many Packets per Second per port are needed to achieve Wire-Speed." [Online]. Available: https://kb.juniper.net/InfoCenter/index?page=content&id=KB14737.

[21] V. Bukac, (2015), "Small scale denial of service attacks," Dissertation. Masaryk University, Faculty of Informatics. Thesis supervisor Václav Matyáš.

[22] Djanie, Tutu, & Dzisi, "A proposed DoS detection scheme for mitigating DoS attack using data mining techniques," Computers, 8(4), 85, 2019

[23] L. Zhou, M. Liao, C. Yuan, & H. Zhang, "Low-rate DDoS attack detection using expectation of packet size," Security and Communication Networks, 2017, 1 -14.