View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 5 (2011) 173–180

Procedia Computer Science

The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT)

Performance Evaluation Study of Intrusion Detection Systems

Adeeb Alhomoud[a]*, Rashid Munir[a],Jules Pagna Disso[a],Irfan Awan[a,b],A. Al-Dhelaan[b]

[a]*IRI,SCIM,University of Bradford,Bradford,BD7 1DP,UK*
[b]*Computer Science,KSU,Riyadh, Saudi Arabia*

Abstract

With the thriving technology and the great increase in the usage of computer networks, the risk of having these network to be under attacks have been increased. Number of techniques have been created and designed to help in detecting and/or preventing such attacks. One common technique is the use of Network Intrusion Detection / Prevention Systems NIDS. Today, number of open sources and commercial Intrusion Detection Systems are available to match enterprises requirements but the performance of these Intrusion Detection Systems is still the main concern. In this paper, we have tested and analyzed the performance of the well know IDS system Snort and the new coming IDS system Suricata. Both Snort and Suricata were implemented on three different platforms (ESXi virtual server, Linux 2.6 and FreeBSD) to simulate a real environment. Finally, in our results and analysis a comparison of the performance of the two IDS systems is provided along with some recommendations as to what and when will be the ideal environment for Snort and Suricata.

Keywords:Attacks; Intrusion Detection Systems (IDS); Traffic; Performance evaluation; Packet drops; Suricata; Snort; Alerts

1. Introduction

Intrusion Detection Systems (IDS) are now becoming one of the essential components in any organization's network. IDS are designed to detect any intrusion or hostile traffic in a network. With the serious need of such detection systems organizations have been investing to produce a more effective IDS. Intrusion Detection Systems can be implemented as a hardware based or software-based [1, 2]. The later type of IDS is more configurable and easy to update while the hardware based is designed to handle large amount of trafficbut more expensive and require more maintenance. There is therefore a need to evaluate the available software-based IDS. In general, instruction detection systems fall into two main categories; Network based systems and Host based systems [3].

Snort is well known and accepted IDS within network security communities and it has been created,developed and maintained since early 1990's. On the other hand, Suricata is part of and funded by the Department of Homeland Security's Directorate for Science and Technology HOST program (Homeland Open Security

* Corresponding author *E-mail address*: a.m.alhomoud@bradford.ac.uk.

1877–0509 © 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
Selection and/or peer-review under responsibility of Prof. Elhadi Shakshuki and Prof. Muhammad Younas.
doi:10.1016/j.procs.2011.07.024

Technology), and by the Navy's Space and Naval Warfare Systems Command (SPAWAR)[4] we have decided to do a live performance evaluation and comparison between the two IDS (the dominant vs. the new).

There have been some few efforts that have been made to measure the performance of IDS. Some of these tests have been using saved data sets rather than real network traffic. Other tests have been using moderate network traffic and/or different IDS system[5, 6]

In this paper we focused on signature-based IDS with an emphasis to evaluate the performance in highspeed network. We aim to provide detailed comparison between the two IDS on three different platforms at highspeed traffic.

This paper is organized into five sections. Section 2 describes the test bench and the component used.Section 3 covers the test scenarios, Section 5.Discuss the results and analysis and finally sections 6 the conclusions.

1.1. Overview of Snort

Snort is well-known name in the information security community as it was created in 1998 by Martin Roeschwho is the founder of Sourcefire and who is still leadingdevelopment of Snort. Snort is an open source network intrusion prevention and detection system (IDS/IPS) that combines the benefits of signature, protocol, and anomalybased inspection. It uses set of rules to check for hostile packets in the network and then generate alerts to the network administrator. The main aim of Snort, Suricata and any other IDS system is to effectively analyze all packets passing throw the network without any packet drops[7].

1.2. Overview of Suricata

Suricata is a rule-based Intrusion Detection/Prevention System (IDS/IPS) that takes advantage of externally developed rule sets to monitor sniffed network traffic and provide alerts when suspicious events take place. Like most IDS it is designed to fit within existing network security components. The initial release of Suricata runs on a Linux 2.6 platform and supports both inline and passive traffic monitoring configuration capable of handling multiple gigabit traffic levels [4]. Suricata works as a multithreaded engine.

According to its creators, the objective of the Suricata Project Phase 1 was to have a distributable and functional IDS/IPS engine. On January 1st,2010 Suricata was made available for download [4].

Suricata is Open Information Security Foundation (OISF)which is part of and funded by the Department of Homeland Security's Directorate for Science and Technology HOST program (Homeland Open Security Technology), by the Navy's Space and Naval Warfare Systems Command (SPAWAR)[4]

2. Test Bench

The network is composed of 8 computers, depending on our need of generating smaller packet size on high traffic speeds. All these computers are connected via ProCurve Series 2900 switch using 1.0 Gigabit Ethernet cable, and two 10 Gigabit cables as shown in Fig.1. The ProCurve Series 2900 switch [8] has been configured to monitor all traffic and send it to the spanning port. This network consists of a high performance PCs (table1) running both open source tools and commercial tools to generate traffic at high speeds and monitor the network performance. We used two 10Gigabit cards one is to be connected the IDS (via monitoring port) while the other one is connected to a high performance pc to generate more traffic as needed. Our selected IDS for this experiment were the latest versions of Snort (v2.9.0.4) and Suricata (v1.0.2).

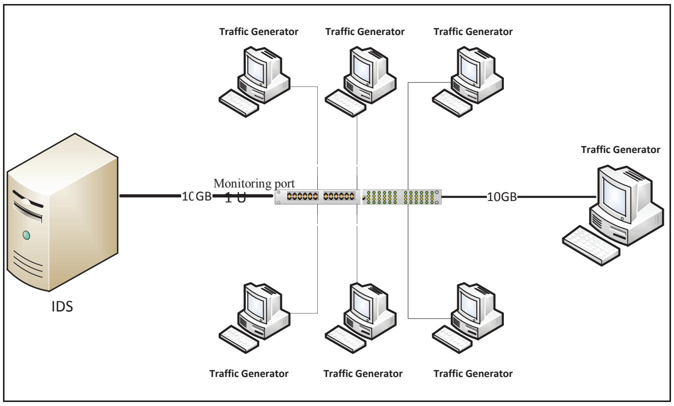

Fig.1Basic network design

The following table (Table 1) shows the hardware specification of the network components.

Table 1. Network components specifications

Machine Type	Hardware Description	Tools used
Windows SP2	Dell Precsion, T3400,Intel Quad-core , Q6600,2GB Ram , 1Gbps network card	LAN Traffic Generator
FreeBSD Linux 2.6	Dell Precsion, T3400,Intel Quad-core , Q6600,2GB Ram , 10Gbps network card	Suricata, Snort Bandwidth monitor
ESXi SERVER	Dell Precsion, T3400,Intel Quad-core , Q6600,4GB Ram , 1Gb network card (for monitoring server), 10Gb for IDS	VMware ESXi Hypervisor Linux 2.6 Suricata, Snort Bandwidth monitor
Attacker	Dell Precsion, T3400,Intel Quad-core , Q6600,2GB Ram , 1Gbps network card	Backtrack Linux Metasploite 3 Framework
Network Switch	ProCurve series 2900	

3. Test scenarios

Test scenarios were designed to test the performance of Suricata and Snort on different operating systems. Both IDS were subject to the same tests and under the exact same conditions. In order to get more accurate results, all scenarios were tested with packet sizes (1470, 1024, 512) for both TCP and UDP. The test was performed for the speed ranging from 250Mbps, 500Mbps, 750Mbps, 1.0Gpbs, 1.5Gbps, and 2.0Gbps. In all the scenarios Suricata and Snort were configured to load and run similar number of rules to monitor. The following subsections will give more view of the test scenarios.

3.1. Scenario A

Most data centers implement the use of virtualization as it is a mean to save time and money. This is a common practice in enterprise environment .In order to ensure the validity of the tests and the accuracy of the comparison of Snort and Suricata, the exact same environment was used for both IDSs.In order to simulate an enterprise’s data center bothSnort and Suricata were implemented on ESXi server [9] . Since this is a performance assessment, all machines should be identical as possible – in terms of hardware - to reflect an accurate comparison. The ESXi server is equipped with 4GB of memory; 2GB was allocated to the virtual Linux running inside the ESXi server. This will make the all IDS machines have the same amount of memory.

Both IDS (Suricata and Snort)were subjected to a heavy traffic on both protocols TCP and UDP, with different packet sizes at different speeds. In order to collect more accurate results, an additional network card was used in the ESXi server toestablish a connection from the management PC to manage the virtual host. The monitoring of the network cards used for the management of the ESXi server has beendisabled from ProCurve switch.

3.2. Scenario B

In this scenario Snort and Suricata were operated on a Linux 2.6 server running Ubuntu 10.10. This machine was configured to monitor traffic using the 10Gbps card.

3.3. Scenario C

Snort and Suricata was operated on FreeBSD server running the latest version 8.1. The FreeBSD has been configured to operate the 10Gbps.

We must clarify that both IDS was ran separately on the platforms allowing it to use all the resources available.

4. Results and Analysis

This section will cover the results and analysis of the performance testsforboth Suricata and Snort on the three different platforms. In order to present understandable results, this section has been divided into two subsections as TCP traffic and UDP traffic. Each subsection will provide a performance comparison between Snort and Suricata performing on virtual machine, Linux 2.6 and FreeBSD handling different packet sizes and speeds.

4.1. TCP

In this section the Snort and Suricata performance on TCP protocol was addressed. Fig 2 illustrates the performance of both IDS systems using the packet size 512. In this test, Suricata was showing some packet drops at early stage (250Mbps) on the Virtual Linux were it reached (35.4%) which is considered very high considering the traffic speed. It also recorded that Suricata has some small packet drops 0.6% on FreeBSD and no packet drops on

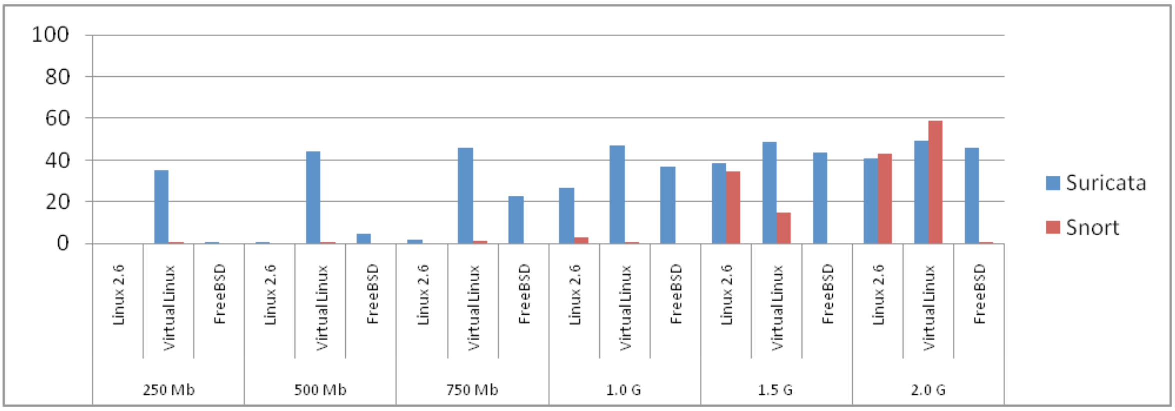

Fig.2 comparison chart of Snort and Suricata (512) TCP

Linux2.6. This percentage of packet drops has increased a little when the traffic reached 500Mbps. On the other hand, Snort was performing very well as there were no packet drops recorded on 250Mbps and 500Mbps on all platforms. Once the speed reached 750Mbps, Snort started to drop some packets but it did not exceed 1.1% on virtual Linux. There was no packet drops recorded on Linux 2.6 or FreeBSD at this speed. At 1.0Gpbs, Suricata was still dropping packets (26.5 on Linux2.6, 36.7% on FreeBSD and 47.2% on Virtual Linux). On Linux 2.6 Snort started to drop packets (2.8%) and only 0.6% on Virtual Linux. No packet drops were recorded on FreeBSD. At the speed of 1.5 and 2.0Gbps, there was a significant decrease in Snort performance as the packet drops exceeded 30% on Linux2.6 and Virtual Linux but no packet drops were recorded on FreeBSD at both speeds (1.5 and 2.0) .

At the packet size of 1024, Fig3, Suricata started recording high packet drops at earlier stage on the Virtual Linux machine. it did not record any packet drops on Linux 2.6. on the other hand, Snort was performing well as no packet drops were recorded on all three platforms at the speeds of 250,500 and 750Mbps. It's worth mentioning that Suricata's performance on Linux2.6 at the speed of 750Mbps is improving as the number of packet loss recorded did not exceed 0.5% on Linux and 6.4% on FreeBSD.

Suricata recorded a high jump in packet drops at 1.0Gbps as it reached 15.7% on Linux, 23% on FreeBSD and 46% on Virtual Linux. On the other hand, Snort was only dropping 0.7% on Linux, 0.56% on Virtual Linux and 0% on FreeBSD. Once the traffic speed reached 1.5Gbps there were significant increases in the packet drops on Linux and Virtual Linux were it hit 27.0%. Suricata at this stage was recording 35% on Linux and more than 48% on Virtual Linux while Snort was recording only 11%.

AT 2.0Gbps, the clear difference in performance was Snort on Virtual Linux as it dropped more than 55% packets were it was only dropping 11% on 1.5Gbps.

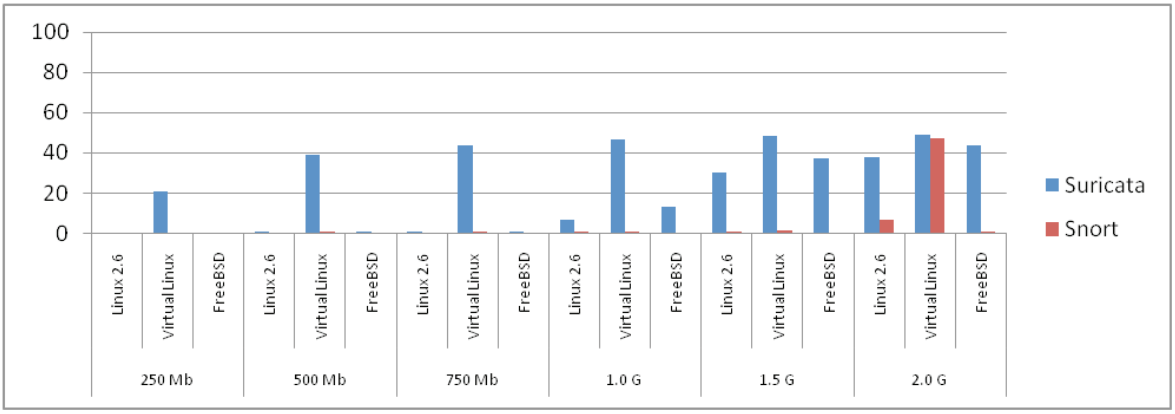

Fig.3 comparison chart of Snort and Suricata (1470) TCP

Fig3 shows the performance of both IDS systems when dealing with a larger pack size. A similar performance to the pervious packet size (1024). The differences in performance started at speeds of 1.5Gbps and above, were the number of packet drops has decreased specially on Snort.

4.2. UDP

As Fig4 illustrates, Suricata was recording some packet drops at a slow speed (250Mbps). This packet drops was recorded when dealing with a packet size of 512. Although there is a high number of packet drops on virtual Linux and FreeBSD, there is no packet drops recorded on Linux. At this speed Snort is performing well with no packet drops on all the platforms. When the generated traffic reached the speed of 500Mbps, Suricata still has a high percentage of packet drops on FreeBSD and virtual Linux, and there is a minor increase in the number of packet loss on the Linux platform. On the other hand, Snort was still performing better than Suricata as no packet drops was recorded on Linux and FreeBSD and only 0.48% on virtual Linux. As can be noticed from the Fig4, Snort made a significant jump in the number of packet drops on Linux2.6 and virtual Linux when the traffic reached 750Mbps.It is worth pointing out that Snort proved to be performing best on FreeBSD as no packet drops were recorded up to this speed.

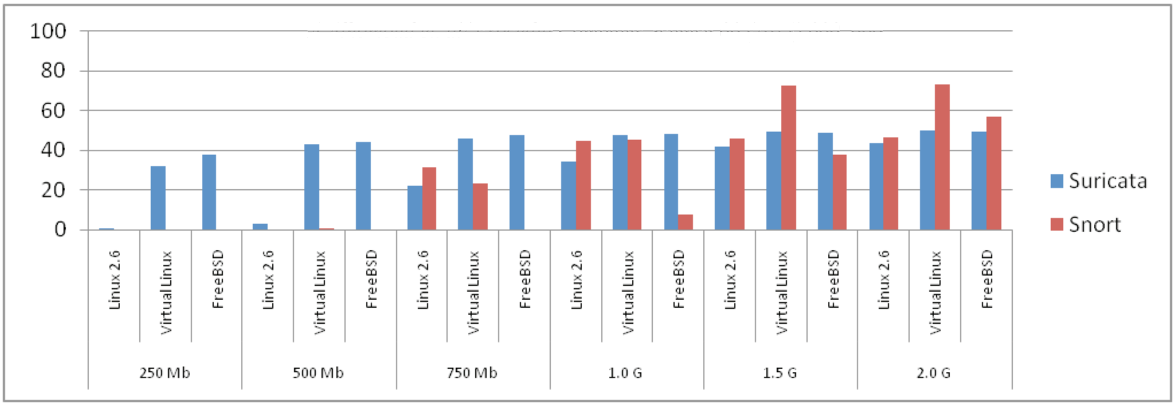

Fig.4 comparison chart of Snort and Suricata (512) UDP

At 1.0Gbps Snort started showing some packet loss on FreeBSD 7.9% and Suricata 45%.When the generated traffic reached 1.5Gbps and above Snort started to drop a high number of packets exceeding more than 73%.

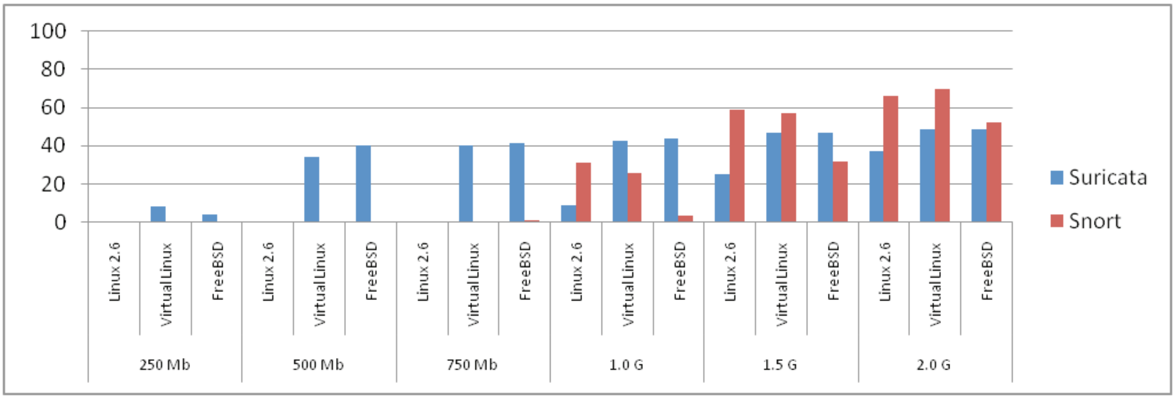

Fig.5comparison chart of Snort and Suricata (1024) UDP

At the packet size 1024 (Fig5) Snort was still a head of Suricata in terms of performance. Snort did not record any packet losses at the speeds of 250 and 500 on Linux and FreeBSD (only 0.1% on Virtual Linux).On the other hand, Suricata reached a high number of packet drops as it reached 40.2% on FreeBSD and 33.9% on virtual Linux. It did not record any packet losses on Linux2.6 at these speeds. Suricata performance at the speeds of 250,500 and 750 was acceptable as it did not exceed 0.33%. The overall performance of Snort at the speed 750Mbps was significantly better on virtual machine and FreeBSD as Snort only recorded 1.2% packet drops.

At higher speeds (1.0Gbps), the best performance was achieved by Snort on FreeBSD with only 3.24% packet drops while the best performance for Suricata was on Linux 8.9%. At the speed of 1.5Gbps and 2.0Gbps both IDSs were dropping a high number of packets.

As can be seen from Fig6, Snort percentage of packet drops is barely noticeable. It can be said that Snort is capable of handling packets of size 1470 well better than Suricata. Snort started dropping packets at the high speed of 1.0Gbps on virtual Linux but did not exceed 1.15% at the speed of 2.0Gbps.

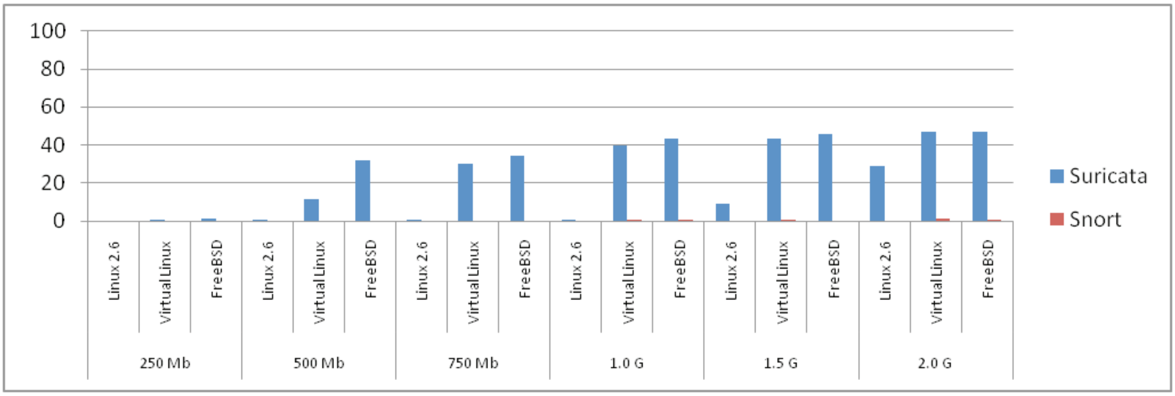

Fig.6comparison chart of Snort and Suricata (1470) UDP

It is worth stating that during the tests we have recorded the CPU usage of both Snort and Suricata on all the three platforms, the following table (Table 2) will show an example of the performance of both IDS systems used along with the CPU utilization. In this example the traffic speed was 1.0Gbps UDP with the packet size of 1024. As it can be seen Snort on FreeBSD uses only 21% of CPU and drops 3.24% while Suricata uses similar CPU usage and drops 43.6%. Suricata performance on the other hand was different on Linux, while it does drops less packets than snort on Linux it uses a high percentage of the CPU 68%.

Table 2.IDSs CPU utilization and packet drops (UDP traffic – Packed size 1024 – 1.0Gbps)

Platform	Snort		Suricata	
	CPU Usage	Packet drops	CPU Usage	Packetdrops
Linux	27%	31.43%	68%	8.9
FreeBSD	21%	3.24%	24.5%	43.6

4.3. Attack detection rate (Alerts)

During the evaluation, attacks have been generated to evaluate the performance of both IDSs in a heavy and mixed traffic. The initial test was perfomed with background traffic only. This was done to confirm that both Suricata and Snort are configured to generate the same number of alerts. We then went on generating the same attacks for both Snort and Suricata in high speeds network.The results are presented in table 3.

Table 3.Percentage of alerts detected

Speed	Snort	Suricata
1.0Gbps	100%	98%
1.5.Gbps	100%	91.8%
2.0Gbps	99.7%	66.8%

5. Conclusions

This paper has focused on determining the efficiency and the performance of the new IDS: Suricata and comparing it to the well know intrusion detection system, Snort, in high speed network environment. Both Snort and Suricata were evaluated on different platforms running on a high performance pcs with different protocols and packet sizes. There are a significant number of packet drops when using virtualization and this is due to the dynamics of virtualization were the allocated physical memory RAM of the host machine is actually an allocated virtual RAM and disk space [6] . This will respectfully affect the performance of Suricata and increases the packet drops as the number of packet received by the network card is higher than what is recorded by the virtual machine this is believed to be due to the bottleneck caused by low disk data transfer[10].

It can be said that Suricata performed well on Linux 2.6 and better than FreeBSD and Virtual Linux but not better than Snort. The following table summarizes the Ideal environment to the IDSs at different speeds.

Table 3.IDSs Ideal operating systems (TCP traffic – Packed size 1024)

Speed	Suricata Ideal platform	Snort Ideal Platform
500	Linux 2.6	Linux 2.6 or FreeBSD
750	Linux 2.6	Linux 2.6 or FreeBSD
1.5	Linux 2.6	FreeBSD
2.0	Linux 2.6	FreeBSD

Table 4.IDSs Ideal operating systems (UDP traffic – Packed size 1024)

Speed	Suricata Ideal platform	Snort Ideal Platform
500	Linux 2.6	Linux 2.6 or FreeBSD
750	Linux 2.6	Linux 2.6
1.5	Linux 2.6	FreeBSD
2.0	Linux 2.6	FreeBSD

As can be seen from the analysis and the summary tables above, Suricata is best implemented on Linux and Snort is best implemented on FreeBSD especially when handling high speeds.

References

1. Bace, R. and P. Mell, Intrusion detection systems. 2001: US Dept. of Commerce, Technology Administration, National Institute of Standards and Technology.
2. Wallner, R., Intrusion Detection Systems. 2007.
3. Di Pietro, R. and L.V. Mancini, Intrusion detection systems. 2008: Springer Verlag.
4. openinfosecfoundation. What is Suricata. Available from: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/What_is_Suricata.
5. Paulauskas, N. and J. Skudutis, Investigation of the Intrusion Detection System "Snort" Performance. Electronics and Electrical Engineering, 2008. 7(87): p. 15-18.
6. Faeiz Alserhani, M.A., Irfan Awan, John Mellor, Andrea J Cullen and Pravin Mirchandani, Multi-tier Evaluation of Network Intrusion Detection Systems. Journal of Information Assurance and Security (JIAS), 2009(1554-1010): p. 301-310.
7. Snort.org. What is Snort?
8. www.hp.com. ProCruve Series 2900 Switch. Available from: http://www.hp.com/rnd/pdfs/datasheets/ProCurve_Switch_2900_Series.pdf.
9. vmware.com. ESXi Hypervisor. Available from: http://www.vmware.com/products/vsphere-hypervisor/overview.html.
10. Akhlaq, M., et al., Virtualization Efficacy for Network Intrusion Detection Systems in High Speed Environment. Information Security and Digital Forensics, 2010: p. 26-41.