ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (1/2017), styczeń-czerwiec 2017, s. 53-65

**Mariusz SZAREK** [1]
**Mariusz NYCZ**[2]
**Sara NIENAJADŁO**[3]

# THE ANALYSIS OF EFFCIENCY AND PERFORMANCE OF INTRUSION PREVENTION SYSTEMS

This article aims at presenting a comparative analysis of two intrusion detection and prevention systems, namely Snort and Suricata, run in the af-packet mode in the context of the efficiency of their protection against the denial of service attacks. The paper sets out, in statistical terms, the denial of service attacks and distributed denial-of-service attacks occurring around the world. In the further part of the research, penetration tests were conducted in order to assess comparatively analysis of the efficiency of IDS/IPS systems was carried out in the context of starting various numbers of network connected devices as well as in the case of sending packets with different sizes. This article is addressed to security systems administrators as well as to people involved in security systems implementation.

**Keywords:** security, network, test, protection, detection, service, denial, intrusion, system, DDoS, DoS, attack

## 1. Introduction

Recent years were marked by the significant progress in the field of devices and ICT technologies in the case of their access to the World Wide Web. This phenomenon is getting more and more dynamic in the last months and years. It has become a regular occurrence that devices such as TV sets, smartphones, tablets and computers are equipped with solutions which enable their users to access the network. The scope of the phenomenon and the research are so significant that the designing and producing have been started of prototypes of other television, radio and household electrical appliances with the capability of network communication. As a consequence of such a widespread digitalization risks and dangers resulting from the use of network devices are growing. These dan-

[1] Mariusz Szarek, Politechnika Rzeszowska, 783535006, 132887@stud.prz.edu.pl
[2] Autor do korespondencji: Mariusz Nycz, Politechnika Rzeszowska, Zakład Systemów Złożonych, mnycz@prz.edu.pl
[3] Sara Nienajadło, Politechnika Rzeszowska, sara.n@op.pl

gers are cyber attacks such as worms, viruses and Trojan horses. They are based on the use of incorrectly programmed or designed applications and devices with security gaps in source codes. These attacks aim at, among others, stealing sensitive information such as personal data of a user/ a company/ an institution as well as at deleting or replacing that data, requesting access to and taking control over the given application/ device/ account/ system or creating the situation when the access to a given service/ assistance is denied. Protection against these types of dangers enhanced to the most is possible thanks to the use of a wide scope of security measures. The advancement, the range and the kind of safety technology used should be determined by the importance and the value of resources and data which are to be protected [17].

Systems, programs, applications and devices developed have security gaps in software and a source code, mainly as a result of an insufficient number of operational tests. The scope of these gaps depends on the type and the advancement of the technology applied. Hackers use these gaps in order to conduct various kinds of cyber attacks. Assistance, support and the automatic update of a code do not provide the comprehensive solution to the problem because the time span between the moment of identifying the weak point in the software and then working out as well as sending a patch by the programmer is long enough to carry out the attack. Together with the growing number of dangers a broad range of solutions is getting more and more available, which not only reduce significantly the risk but also happen to eliminate it completely from time to time.

At present, Denial-of-Service attacks (DoS) and Distributed Denial-of-Service attacks (DDoS) are extremely popular. The attacks are intended to block the possibility to use and administer web servers of various types of companies and institution, namely websites of non-governmental organizations, self-governing and scientific bodies, and websites of banks, shops and web portals. Attacks result in the huge increase of delay times of particular sites or, in the worst case, in the complete standstill. Successful attack on a given web site can cause the loss of trust of customers and users connected with this institution, which can in turn considerably affect the financial performance. DoS attacks are used for political and terrorist reasons in order to block systems and web sites which a crucial for a state.

There is a wide variety of solutions which protect the respective network's and information systems' components against DoS and DDoS attacks. It is recommended for instance to use only essential and necessary programs, applications and services. Access lists at routers and firewalls are created and configured. The use and accessibility of hardware and computational resources as well as CPU utilization are monitored on a continuous basis. Network capacity limits are introduced. Administrators and users are forced to write long and complex passwords which include capital and lower case letters, digits and special cha-

racters. They are also obliged to change passwords very often. Frequent, regular and automatic firmware updates are performed in order to eliminate gaps in the software. Frequent and systematic backup copies of company's data are made. In the case of the attack tools are used which enable to target a type and source of this attack and, furthermore, cause the immediate cut-off of a network and devices from the source.

Intrusion Detection Systems and Intrusion Prevention Systems are among the most modern, the most efficient and the most common tools used to protect against Denial-of-Service attacks and Distributed Denial-of-Service attacks. There are two of IDS/IPS systems – physical (hardware) and logical (software). They are used to detect and also react to attack attempts on networks, systems, and network devices in the case of IPS systems. Many global companies from the IT security and computer network branch produce physical solutions, which are expensive to buy and to operate and for this reason used only in the largest companies and institutions. Free programming solutions, which base their operations on packet lines, are used widely.

## 2. The Presentation of Denial-of-Service attacks

### 2.1. Definition and Types of Denial-of-Service Attacks

Denial-of-Service attacks are specified as cyber attacks which aim at making a given service or a computer system stop working as a result of a saturation of hardware or computational resources. These are the most frequent, the most productive and the most effective cyber attacks. There is a high variety of techniques, solutions and ways of denial-of-service attacks, which are used by hackers according to the objective pursued, and its advancement and complexity. As an example, the Denial-of-Service attack is the transmission of an enormous number of packets to the victim's environment in order to occupy all the resources available and as a result to cause the device or a system malfunction due to overload. The use of security loopholes in particular protocols of ISO/OIS model layers is one the other way employed by attackers. Denial-of-Service attacks are characterized by the fact one does not need huge financial push, extraordinary amount of time or expensive devices in order to conduct them and, what is more, the structure of the attack is not complicated as well. Due to the aforementioned factors, Denial-of-Service attacks are growing in frequency, complexity and advancement. Hackers draw up and create new, innovative and increasingly complex forms, ways, types, techniques and methods of these attacks. The fowing diagram presents Denial-of-Service attacks which occurred [1][2] (Fig. 1).

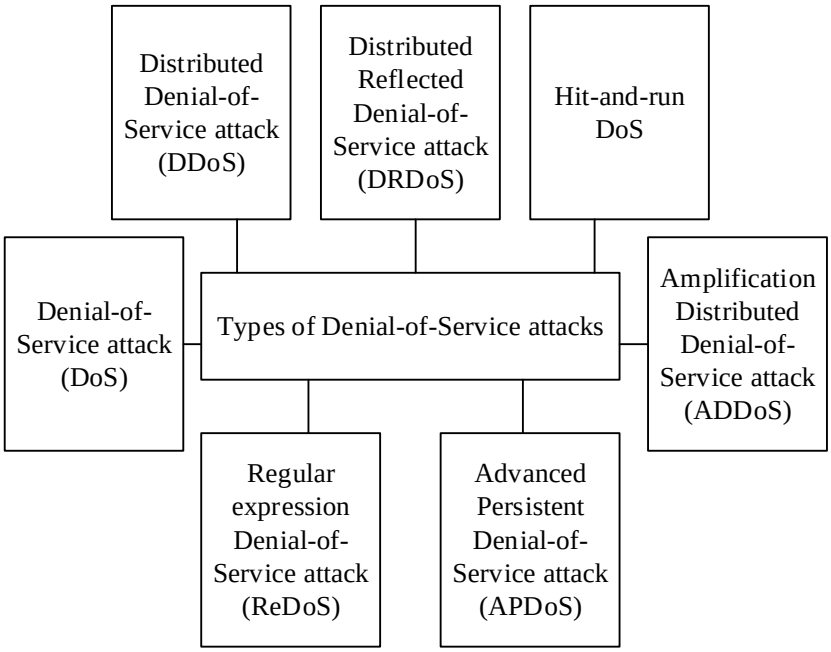


Fig. 1. Types of existing Denial-of-Service attacks [1] [2]

## 2.2. The statistics of existing Denial-of-Service attacks around the world in the fourth quater of 2016 and first quarter of 2017

Companies, which produce solutions to protect data, resources, servers, devices and network services against cyber threats, conduct research and compile statistics that enable them to evaluate existing dangers more efficiently and also fight with these threats. The aggregated results of research and statistics define the trends of existing dangers in the event of cyber attacks which will make it possible to create new hardware and software solutions for ensuring protection as well as improve the existing ones.

Each quarter, Akamai company presents results of research devoted to the occurrence of Denial-of-Service attacks around the world. According to the report from the first quarter of 2017 the fragmentation of UDP packets was the most frequent cause of Denial-of-Service attacks around the world since it adds up to 29% of all the dispersed Denial-of-Service attacks conducted in the first quarter of 2017. Among other frequent attacks are those directed at protocols NTP, DNS, SYN segment as well as UDP flood. The graph below shows the frequency of particular targets of DoS and DDoS attacks in the first quarter of 2017 [3] (Fig. 2).

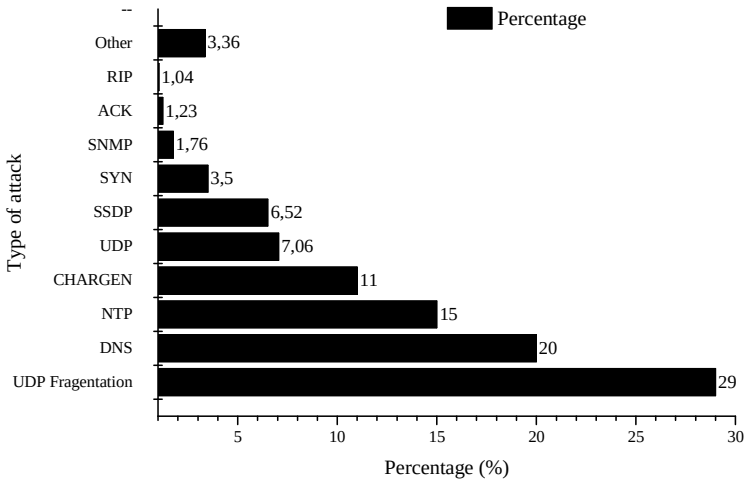


Fig. 2. Percentage summary of the types of DoS and DDoS attacks which took place around the world in Q1 2017 [3]

Furthermore, the report of Akamai company presents a league of countries where web application attacks took place most often in the first quarter of 2017. U.S. has been ranked first in this evaluation. 221 million of the attacks happening in the first quarter of 2017. Countries such as Brazil, U.K., Japan and Germany noted much less of the web application attacks. The graph below shows a league table of countries where web application attacks were most frequent in the first quarter of 2017 [3] (Fig. 3).

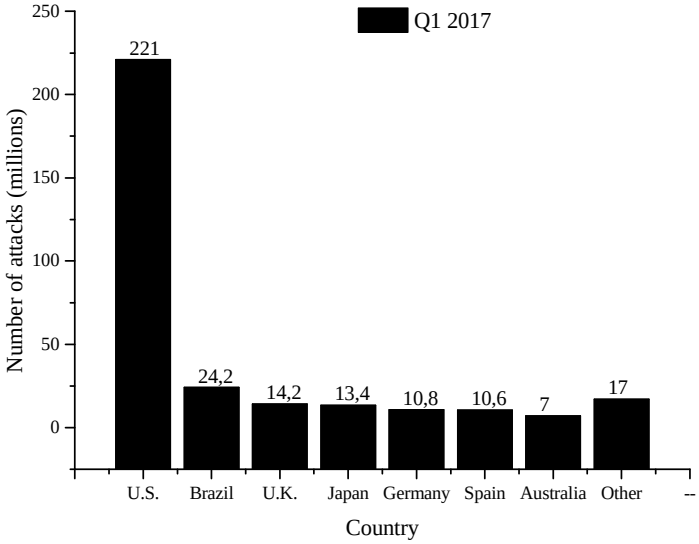


Fig. 3. Top Source Countries for web application Attacks, Q1 2017 [3]

The following graph presents frequency of web application attacks which took place in first quarter of 2017 (Fig. 4). The most popular type of attack is SQL injection, with 44% of all attacks. On the second place is LFi taking up 39% of web application attacks. The third place occupies XSS with 10% of all web application attacks [3].

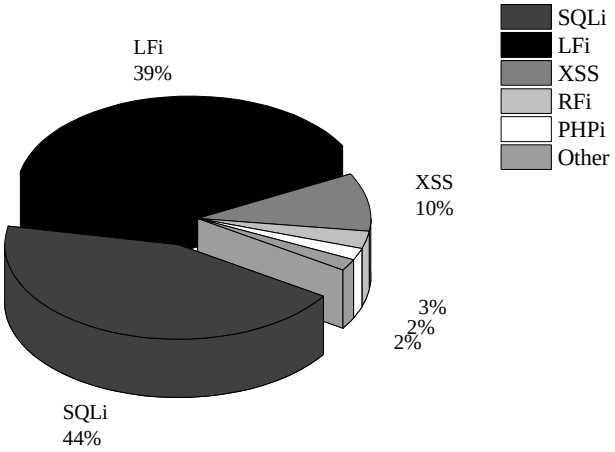


Fig. 4. Web Application Attack Frequency, Q1 2017 [3]

## 3. The Analysis of Efficiency nad Productivity of IDS/IPS Snort and Suricata Systems run in the af-packet mode when faced with DoS AND DDoS attacks

Intrusion Detection Systems and their extension, namely Intrusion Prevention Systems are an efficient and widely used way of fighting against threats connected with Denial-of-Service attacks and other cyber-attacks. Their objective is to maximalise in real time the safety of administrators and users of particular systems, applications and Web services against attacks through the implementation of specifically designed physical (hardware) and logical (software) solutions [4].

Intrusion Detection Systems are used to identify unauthorized and unwanted system or computer network invasion. They are highly specialized tools such as devices, applications and services executed on electronic equipment connected with the network. These systems monitor the network in real time in order to detect possible risks, dangerous elements, components, events and in order to break security policy rules of a given electronic system. Founding this dangerous element result in creating the message stored in a database or in a source file. The most important in the process of working out the intrusion detection system is the implementation of solutions which enable system to operate automatically

without the constant control of an administrator, a user. Such solutions make it possible to modify in real time options and properties of a firewall. These solutions allow to eliminate almost completely the occurrence of the attack which use vulnerabilities in a source code [4-6].

Intrusion Prevention Systems are extensions of IDS systems with mechanisms which prevent breaking into by rejecting packets with malware sent to a victim of an attack. These mechanisms are added to properties, functions and features of IPS systems. Appropriate library must be added to a system and this system must be placed on the packet line so that system IDS will be able to work efficiency as IPS system [4].

The effectiveness analysis of IDS/IPS systems in the context of the protection against Denial-of-Service attacks was conducted with the example of two free-of-charge programming systems IDS/IPS Snort and Suricata which run in the af-packet mode.

### 3.1. The description of configured and used test environment

IDS/IPS Snort and Suricata systems which are run in the af-packet mode were analyzed in terms of their effectiveness concerning the protection against dispersed Denial-of-Service attacks: SYN-Flood and Land [7-10].

The test environment comprising of three virtual machines with Debian system and IDS/IPS Snort and Suricata systems were prepared to cater the needs of simulation and research. These machines carried out the functions of machines under attack. Moreover, the test configuration comprises of attacking environment, namely the virtual machine with Kali Linux system installed. Open source packets generator hping3 was installed on this system, which was used to simulate attacks. Apart from attacking machines and the machines under attack there was also a router in the network which provided connection between virtual machines and Internet [11-16].

### 3.2. Research and comparison of the effectiveness of IDS/IPS systems run in the af-packet mode in the context of the protection against Denial-of-Service attacks concerning SYN-Flood and Land

Initially, tests were conducted on the machine of a victim in the situation when there was no IDS/IPS system operating in the environment of the victim. Research was conducted with various numbers of terminals switched on when SYN-Flood attack was up and running in the attacking environment. This graph below shows response time during communications between different network entities in case of SYN-Flood attack on the Network without any of the IDS/IPS systems operating (Fig. 5).

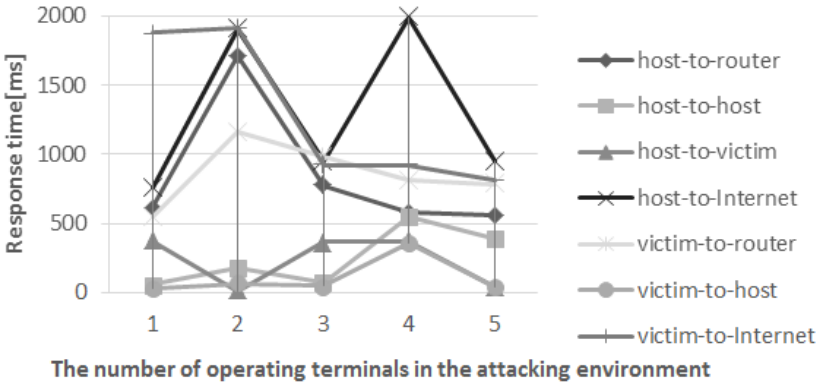


Fig. 5. Response time during communication between respective network entities in case of Land attack on the system without any of the IDS/IPS systems operating

Next testing phase was based on researching the response time of particular network entities in situation when IDS/IPS Snort and Suricata systems run in the af-packet mode. The research was conducted with various numbers of switched on terminals when SYN-Flood attack was conducted in the attacking environment. The graph below shows response time during communication between different network entities in case of SYN-Flood attack on the network with Snort system run in the af-packet mode (Fig. 6).

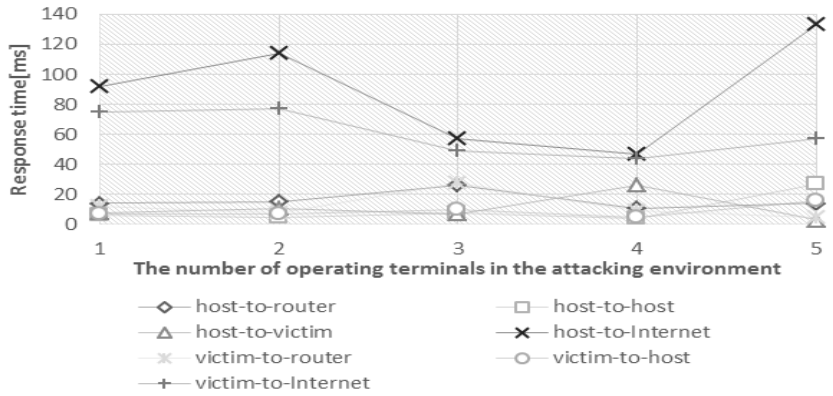


Fig. 6. Response time during communications between different network entities in case of SYN-Flood attack on the network with Snort system run in the af-packet mode

The graph below shows response time during communication between different network entities in case of SYN-Flood attack on the network with Suricata system run in the af-packet mode (Fig. 7).

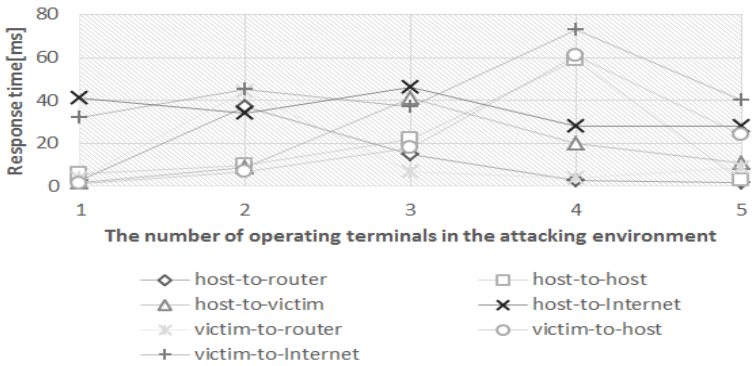


Fig. 7. Response time during communications between different network entities in case of SYN-Flood attack on the network with Suricata system run in the af-packet mode

Land attack was the second Distributed Denial-of-Service attack which was examined in the research. As in the case of SYN-Flood attack, first one examined delay time during communications between particular network entities in case when there was no IDS/IPS system operating. Research was conducted with various numbers of terminals switched on when Land attack was up and running in the attacking environment. This graph shows response time during communications between different network entities in case of Land attack on the network without any of the IDS/IPS systems operating (Fig. 8).

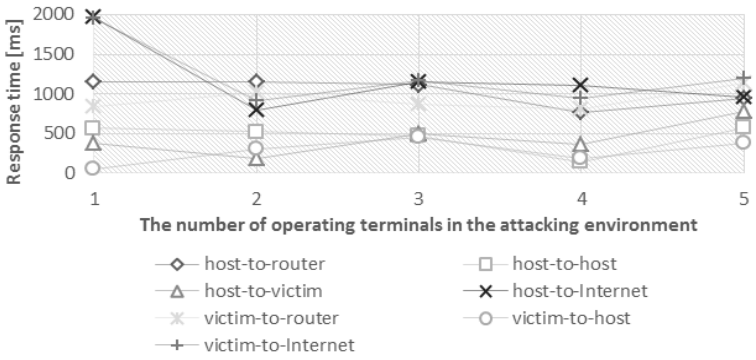


Fig. 8. Response time during communications between different network entities in case of Land attack on the network without any of the IDS/IPS systems operating

Similarly to SYN-Flood attack, next testing phase was based on researching the response time of particular network entities in situation when IDS/IPS Snort and Suricata systems run in the af-packet mode. Research was conducted with various numbers of terminals switched on when Land attack was up and running

in the attacking environment. The graph below shows response time during communication between different network entities in case of Land attack on the network with Snort system run in the af-packet mode (Fig. 9).

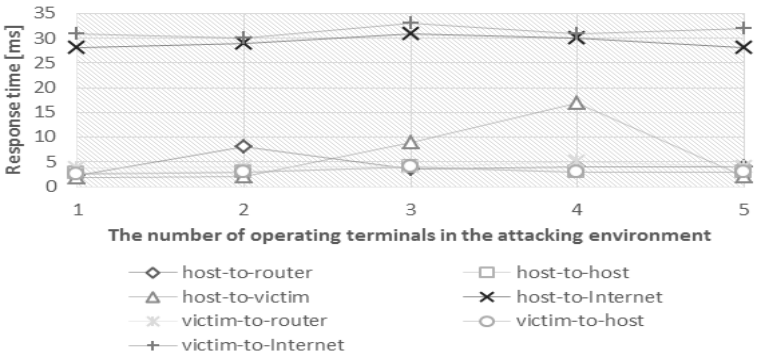


Fig. 9. Response time during communications between different network entities in case of Land attack on the network with Snort system running in the af-packet mode

The graph below shows response time during communication between different network entities in case of Land attack on the network with Suricata system run in the af-packet mode (Fig. 10).

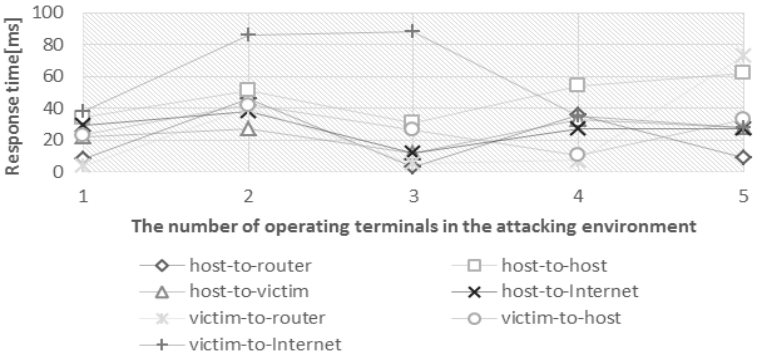


Fig. 10. Response time during communications between different network entities in case of Land attack on the network with Suricata system run in the af-packet mode

### 3.3. The efficiency tests of IDS/IPS Snort and Suricata systems with regard to response time depending on the number of served hosts and on the size of transmitted packets

A part from the tests of IDS/IPS systems in the context of the efficiency of their protection against Denial-of-Service attacks and Distributed Denial-of-

Service attacks, the productivity analysis of these systems was also carried out. To this end, delay time was examined during packet transmission on a line host-router in case of various numbers of hosts served by IDS/IPS system. The graph bellow shows delay time in communication between a host and a router with Snort and Suricata system running in the af-packet mode when these systems serve various number of network devices (Fig. 11).

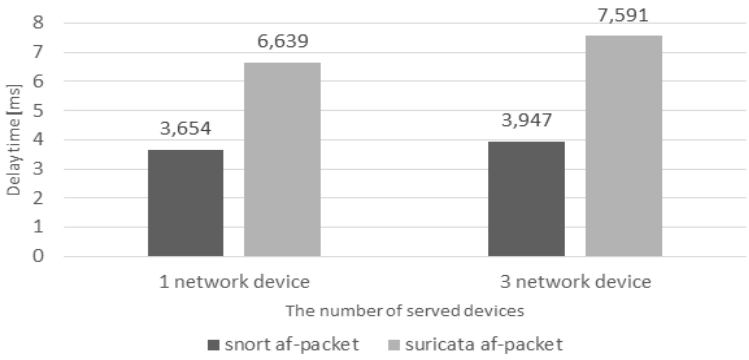


Fig. 11. Delay time in communication between a host and a router with Snort and Suricata system running in the af-packet mode when these systems serve various number of network devices

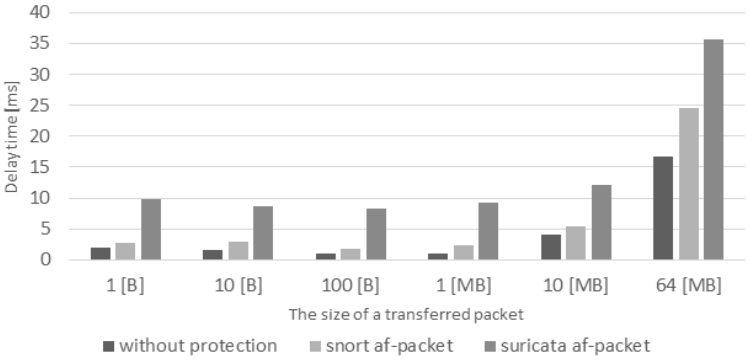


Fig. 12. The comparison between delay time during the transmission of packets having various sizes between a host and a router when there is no IDS/IPS system operating, when Snort system is running in the af-packet mode, when Suricata system is running in the af-packet mode

The second efficiency test of IDS/IPS Snort and Suricata systems consisted in the observation of delay time during the transmission of packets having various sizes between a host and a router when the systems were switched on. The graph below presents delay time during the transmission of packets having va-

rious sizes between a host and a router when there is no IDS/IPS system operating, when Snort system is running in the af-packet mode, when Suricata system is running in the af-packet (Fig. 12).

## 4. Summary

The research conducted proved that IDS/IPS Snort and Suricata systems run in the af-packet mode are efficient in protecting devices, resources and network entities against Land attack which belongs to the group of Denial-of-Service attacks. The start of both these systems causes the significant reduction in response time during communications between various network entities, which leads to the uninterrupted use of network services. As far as SYN-Flood is concerned, Suricata is slightly more efficient with delay time not exceeding 80 [ms], but in case of Land attack Snort system is more efficient with response time not exceeding 35 [ms]. On the basis of results obtained one can claim that both Snort and Suricata run in the af-packet mode are protecting the network effectively against Denial-of-Service attacks and Distributed Denial-of-Service attacks. The productivity tests show that Snort system is more productive than Suricata system, because regardless of the number of hosts of the size of transmitted packets, response time when this system is operating is lower than response time when Suricata system is switched on. Both is case of Snort and Suricata system the increase in the number of hosts served does not cause the significant increase in response time. The size of transmitted packets is of almost no importance to the efficiency of IDS/IPS systems on condition that packets transmitted are of low (up to 1[MB]). The transmission of huge packets (more than 1[MB]) cause the significant increase in responses during communication between particular network elements when IDS/IPS systems are operating.

### References

[1] https://dataspace.pl/dos-rodzaje-atakow-cz-1/[Access: 24.08.2015]

[2] https://dataspace.pl/dos-rodzaje-atakow-cz-2/[Access: 3.09.2015]

[3] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-security-executive-summary.pdf [Access: 19.05.2017]

[4] K. Scarfone, P. Mell: Guide to Intrusion Detection and Prevention Systems (IDPS)

[5] http://students.mimuw.edu.pl/SO/Projekt04-05/temat5-g2/sikora-kobylinski/idsips.html [Access: 23.12.2015]

[6] http://sekurak.pl/wprowadzenie-do-systemow-ids/[Access: 23.03.2015]

[7] http://insecure.org/sploits/land.ip.DOS.html[Access: 20.11.1997]

[8] http://www.computerworld.pl/news/291980/Atak.na.sieci.IP.html [Access: 29.12.1997]

[9] https://www.incapsula.com/ddos/attack-glossary/http-flood.html [Access: 18.10. 2015]
[10] https://www.incapsula.com/ddos/attack-glossary/syn-flood.html [Access: 18.10. 2015]
[11] https://www.debian.org/doc/ [Access: 7.04.2015]
[12] https://www.snort.org/documents/snort-ips-tutorial [Access: 25.08.2015]
[13] https//www.snort.org/documents [Access: 25.08.2015]
[14] https://www.kali.org/kali-linux-documentation/ [Access: 2.01.2016]
[15] http://wiki.hping.org [Access: 30.09.2009]
[16] http://suricata-ids.org/docs/ [Access: 6.08.2014]
[17] Ch. Chapman: Network Performance and Security: Testing and Analyzing Using Open Source and Low-Cost Tools

## BADANIE SPRAWNOŚCI SYSTEMÓW IDS/IPS PRZED ATAKAMI DOS I DDOS

**S t r e s z c z e n i e**

Tematem artykułu jest analiza sprawności systemów wykrywania i zapobiegania włamaniom przed atakami odmowy usługi. W początkowej cześć artykuł w oparciu o wynik analiz, zaprezentowano skalę problemu omawianych zagrożeń. W kolejnych paragrafach przedstawiono metodykę badań określenia podatności na ataki odmowy usługi. Następnie przeprowadzono symulacje wydajności i skuteczności obrony przed atakami dwóch sieciowych systemów wykrywania włamań w segmencie open-source Snort i Suricata. Analizowano rozwiązania pracując w trybach nfqueue i af-packet, przy zestawie tych samych reguł. Przeprowadzone testy porównawcze z wykorzystaniem dwóch najpopularniejszy zagrożeń tj. Land i SYN Flood, wykazały przewagę rozwiązania Suricata w skuteczności wykrywania analizowanych ataków. Artykuł jest adresowany do osób zajmujących się wdrażaniem i administracją systemów zabezpieczeń.

**Słowa kluczowe:** sieci, bezpieczeństwo, ochrona, testy, odmowa, usługi, wykrywanie, wtargnięcie, przeciwdziałanie

DOI: 10.7862/re.2017.5

*Tekst złożono w redakcji: maj 2017*
*Przyjęto do druku: czerwiec 2017*