Internal Threat Defense using Network Access Control and Intrusion Prevention System

Andhika Surya Putra[1], Nico Surantha[2]
Computer Science Department, BINUS Graduate Program–Master of Computer Science
Bina Nusantara University, Jakarta, Indonesia 11480

***Abstract*—This study aims to create a network security system that can mitigate attacks carried out by internal users and to reduce attacks from internal networks. Further, a network security system is expected to be able to overcome the difficulty of mitigating attacks carried out by internal users and to improve network security. The method used is to integrate the ability of Network Access Control (NAC) and the Intrusion Prevention System (IPS) that have been designed and implemented in this study, then an analysis is performed to compare the results of tests that have been carried out using only the NAC with the results using integration of NAC capabilities and IPS. The results obtained from the tests that have been carried out, namely, the security system by using the integration of NAC and IPS capabilities is better than using only the NAC.**

***Keywords*—Attack; integration; Intrusion Prevention System (IPS); mitigation; Network Access Control (NAC); network security**

I. Introduction

For decades, technology plays an important role in most activities. Most organizations use technology to support their business processes. Nowadays, internet is used for almost all activities especially business activities. Thus, network infrastructure plays a vital function in an organization. Most organizations are connected to the internet to make all information easily accessed from anywhere and anytime. Network can also be considered as a major risk for an organization. Today's advancement of IT technology bring to the surface the issue of security. Thus, it is important to secure the network infrastructure [1] [2]. In the operation of network can be compromised by any vulnerability in their functionality to attack the networks. Some mechanisms are widely used to secure the network, namely Intrusion Detection System (IDS) that has the ability to detect malicious and unauthorized activities and Intrusion Prevention System (IPS) that has the ability to make an action for detected intrusion [3] [4] [5]. The purpose of using IDPS is to monitor and protect attacks from intruder who want to enter the system, and then give a report to the network administrator if there are attacks that occur in the network environment [6] [7]. So, using IDPS can help to detect and carry out security against intrusions that occur on the network.

Attack threats can be caused by either outsiders or insiders in an organization. Insider attacks are malicious attacks carried out on networks or computer systems with authorized/official system access [8] [9]. Insider attack is one of the most difficult threats to be detected because (IDS) is built to defend against outside attacks [10]. Generally, IPS is placed in the edge of a network, it is done so to avoid incoming intrusion flows from the outside [11]. Thus, concerns that attacks can still arise from inside intruders to network before reaching IPS still exists in the network. Therefore, a network security is needed from the lowest level of the internal network as well.

Network Access Control (NAC) is an approach designed to increase network security by controlling the access and the resources for legitimate users [12]. NAC not only allows network access requested by the user, but also provide specific access based on the user's identity [13]. One of the threats to enterprise networks is the personal devices of employees and guests that do not have anti-virus, patches or host intrusion prevention system in place. An NAC solution can protect a network from such end devices and detect and rectify these problems [14]. NAC function has certain weaknesses, in particular it is unable to detect and stop users that have legitimate network access form carrying out intentional or unintentional attacks from within. Example of intentional attack is when an internal user has a desire to destroy the internal system due to personal problems, whereas unintentional attacks can happened through downloading files or applications that contain malware or viruses. This condition can happen because NAC does not have the ability to detect attacks like IPS.

Based on the weaknesses of the NAC, there is a need to improve network access security from within. In this research, a solution is proposed to improve network security from internal sides of the network by integrating NAC and IPS capabilities. The benefits obtained from this solution can minimize the threat of attacks on the network.

II. Review of Related Literature

A. NAC

NAC systems combine endpoint security solutions to grant access control and enforce security rules or policies to every device connected to the network. The NAC policy is able to identify endpoints that are connected to the network. This policy is carried out to restrict access of devices that do not comply with predetermined network access rules [15]. NAC also provides security and control for those who have access to networks and resources within the network. Basically, NAC performs posture, quarantine, and remediation checks involved in requests for network access by users. If the user does not have the appropriate posture in his computer such as the latest OS/security patch or the most updated antivirus, then the user will not be allowed to enter the network, but the user will be

quarantined by being separated into different networks or VLANs until the user performs a remediation process to meet the requirements needed for entry into the network [16] [15].

Some reasons for using the NAC solution are: to identify and authenticate users and endpoints, to limit user access to the network, to limit access based on the endpoint security posture, and to remediate an endpoint if the endpoint does not have a posture that complies with the provisions [17]. Another reason for implementing the NAC is due to the threat that comes from using your own device (BYOD) approach. With many users using their own devices to work and use them for work purposes, NAC is increasingly needed because many security threats might occur due to devices that do not have enterprise-level device security standards such as patch OS and antivirus.

Comparative studies of existing NAC systems has concluded that the NAC solutions from Cisco, Trustwave, and Forescout can be implemented in accordance with the existing network infrastructure so that it can produce maximum profits where NAC can limit the access of devices and users that are defined based on existing roles and ensure network access obtained according to what is needed [17]. The main benefit of NAC systems is to prevent potentially malicious or infected devices from entering the network in order to keep the network clean [18]. So that network security can be increased from the user level by using NAC.

B. IDS and IPS

There are a couple of widely used mechanisms to secure the network, namely Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Intrusion detection is the process of monitoring events on a network or computer system and analyzing them for possible threat incidents and violations of standard computer security practices, usage policies, or security policies [3]. IDS is a hardware component or software that automates the intrusion detection process. It monitors events that occur on network and computer systems and responds to alert with an indication of potential network security policy violations [19] [20]. IPS is a network device or software that identify and block network threats by assessing each and every packet based on the network protocols in the network layer, tracking each session. Intrusion Prevention System is a defense mechanisms designed to detect malicious packets within network traffic and stop intrusions, blocking the aberrant traffic automatically before it does any [3] [21]. IPS is an improvement from IDS because it does not only have the ability to detect intrusion, but also can take action against intrusion or potential malicious network activity [22] [23].

There are several approaches that have been carried out by previous researchers. The objective to be achieved in their research is to evaluate and analyze the performance of NGIPS in securing networks through penetration tests using HTTP ports, so that the inspection and protection performance of NGIPS is known. The benefit of this research is that it can be a point of reference in improving network security using the NGIPS method and to obtain optimal mechanism for implementing NGIPS. Based on the results of these penetration tests, it proves that NGIPS can save attacks that exploit vulnerabilities from HTTP ports [24]. By using IPS, attacks that cannot be detected by a firewall and NAC can be detected properly and therefore increase network security.

III. Methodology

A. System Design

As summarized in Table I, IPS used in this study is products from Cisco, Cisco FirePower 8250 with OS 6.2.3 series. The IPS has been connected between a firewall device and core switch. Using the NAC system from Cisco requires a Cisco NAC device called the Cisco Identity Service Engine (ISE). Cisco ISE is a Cisco appliance used for NAC systems. The ISE will be linked and integrated with existing network infrastructure devices such as switches and radius servers to authenticate. Physically, the Cisco ISE will be connected to the server-farm switch. This is done so that Cisco ISE can be integrated with all segments in the network infrastructure. The hardware of Cisco ISE used is appliance with SNS 3495 type and the OS version of Cisco ISE used is ISE 2.3. The NAC will be able to communicate with IPS to carry out the expected integration in accordance with the objectives of this study. The access switch that directly connected to the user's PC uses Cisco Catalyst 2960X with 15.2(2)E7 IOS version. The computer used as an attacker and the target is HP ProOne 600 using windows 10.

Fig. 1 below proposes a new topology using Cisco FirePower and Cisco ISE connected to the network. In this study, the device was integrated with existing infrastructure. The integration carried out in this study is physical and logical connection where the Cisco ISE NAC and IPS Cisco FirePower must be able to connect with existing infrastructure devices, change server farm connections from core switch through IPS, configure to integrate between the Cisco ISE NAC, IPS Cisco FirePower and existing infrastructure devices, as well as making policies and rules on the Cisco ISE NAC and IPS Cisco FirePower to achieve the objectives in this study which are to create a network security system that can mitigate internal users who carry out attacks and to reduce attacks from internal networks by using NAC and IPS system integration.

B. Implementation and Testing

In this study, tests were carried out to prove the solution given to address the existing problems. These tests were carried out by using a system and infrastructure design that has been integrated with the NAC and IPS systems. The tests took place by trying to connect an internal user PC to the internal network with the Windows 10 operating system which acted as an attacker, placing the target server connected to the firewall using workstations with vulnerable OS installed. Then, worked on the IPS and NAC configuration so that the two systems can communicate and integrate in order to achieve the objectives of this study.

TABLE. I. System Specifications

Device	Vendor	OS Version
PC	HP ProOne 600	Windows 10
Access Switch	Cisco Catalyst 2960X	15.2(2)E7
NAC	Cisco ISE SNS 3495	2.3
IPS	Cisco FirePower 8250	6.2.3

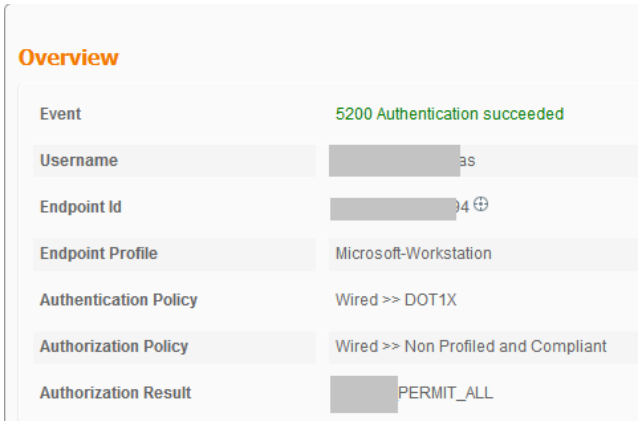

Fig. 1. User Compliant Status on NAC.

In this test, the IPS is located in the middle of a network that is configured inline so that the IPS can immediately make decisions on packages that have been inspected. The package is analyzed by the IPS based on its signature. If the package contains crime or vulnerability, the IPS will immediately prevent it by blocking the malicious package. Then, the IPS provides information on the source of the attack to the NAC so that the NAC can immediately prevent and quarantine the computer that is the source of the attack so that it cannot launch attacks again on the network. In this test, there were two types of users, a compliant user which is an official network access condition with certain requirements and a noncompliant user which is an unofficial network access condition because the user does not comply with the specified requirements. Screening tests were conducted by using several legitimate traffic samples such as HTTP and SSH as well as malicious traffic such as sql injection and os bash injection.

IV. Result and Discussion

A. Compliant user with Legitimate Traffic

In the test, the computer used by a compliant user tried to access the network by physically connecting the cable from the PC to the access switch. The PC user is considered compliant by the NAC because it complies with the specified requirements such as a join domain and has anti-virus as shown in Fig. 2. Then the user tried to access legitimate HTTP traffic to the server with the vulnerable OS used in this study successfully as shown in Fig. 3. Afterward, the user tried to access legitimate SSH traffic to the server with the vulnerable OS used in this study successfully as shown in Fig. 4. Comparing the result of legitimate HTTP and SSH traffic by using only the NAC with the one using integration of the NAC and the IPS, the result is similar that the user can access any legitimate HTTP and SSH traffic.

B. Compliant user with Malicious Traffic

Based on tests, the computer used by a user tried to access malicious traffic with sql injection attack. The attack used “hi’ or 1=1--” command on login field in web browser that aimed to trick sql server to bypass the login on the server. With only using the NAC, this attempt succeeds to bypass the website login with the sql injection command as shown in Fig. 5. This can be done because the NAC cannot detect the sql injection attack as the NAC only knows that the attacker is a compliant or authorized user. But by using integration of the NAC and the IPS, the sql injection attempt was detected and blocked by the IPS. The IPS instructed the NAC to quarantine the infected user immediately, so the user cannot do any more attack because the NAC is blocking the attacker connection via the access switch as shown in Fig. 6.

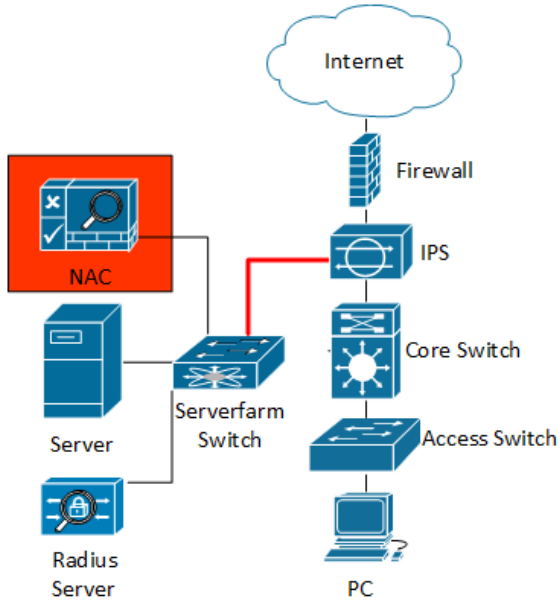

Fig. 2. Proposed Network Topology.

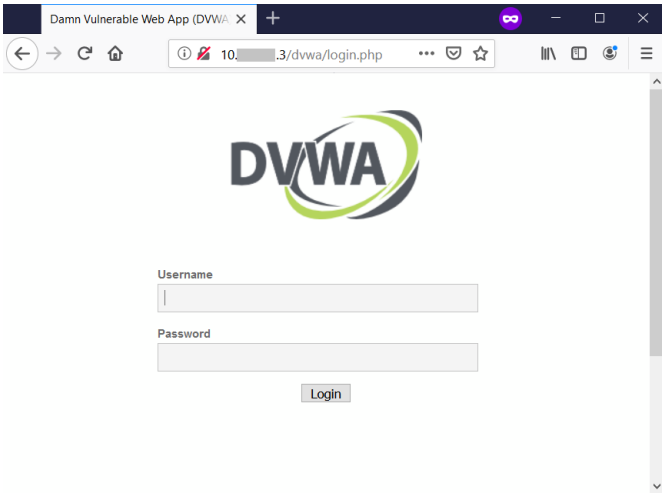

Fig. 3. Compliant user Legitimate HTTP Traffic.

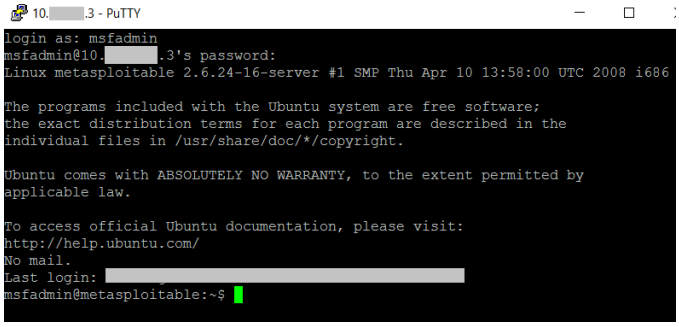

Fig. 4. Compliant user Legitimate SSH Traffic.

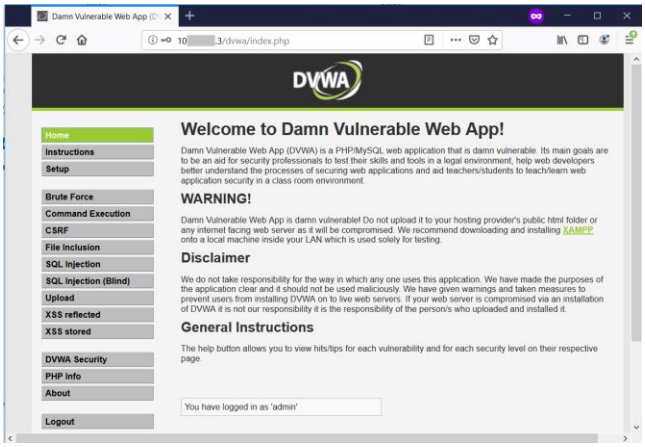

Fig. 5. Successful Login using Sql Injection Attack.

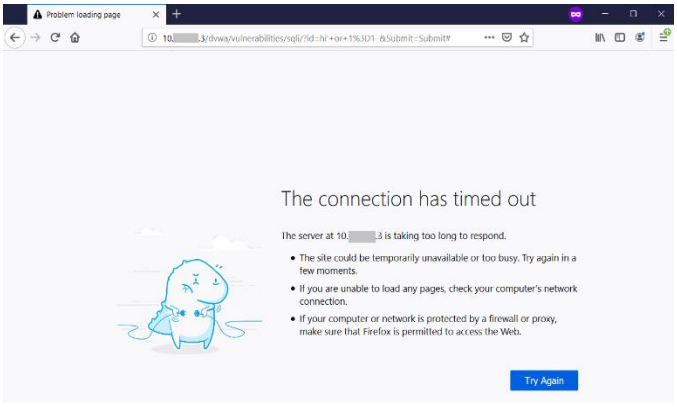

Fig. 6. Blocked Attacker Network Access by NAC.

The second malicious attempt used is through os bash injection. Os bash injection attacks were carried out on the target server by using the vega vulnerability scanner tool on the attacker's computer. Run the vega tools then run a scan to test the os bash injection attack as shown in Fig. 7. With only using the NAC, the attempts still succeed to launch attacks to the targeted vulnerable server. But by using integration of the NAC and the IPS, the os bash injection attempt was detected and blocked by the IPS. The IPS instructed the NAC to quarantine the infected user immediately, so the user cannot do any more attack because the NAC is blocking the attacker connection via the access switch as shown in Fig. 8.

C. Noncompliant User

A user is deemed noncompliant by the NAC because the user does not pass the required NAC system, the user cannot get any network access and mitigated by the NAC by denying the network access for the user as shown in Fig. 9. Therefore, user cannot go through with either malicious traffic or even legitimate traffic as they have no access to the network.

Table II summarized the results based on the tests that have been completed for this study. It shows significantly different results in treating compliant users who commit malicious traffic on the network only with the NAC with the one using the proposed solution of integration between the NAC and the IPS. The expected test results in this study can be achieved by using the proposed solution. The proposed solution shows that by integrating capabilities of the NAC and the IPS can mitigate attacks from internal users and can reduce attacks from internal networks by 40% based on the test scenarios performed. Therefore, integration of the NAC and the IPS can increase network security compared to the use of NAC alone.

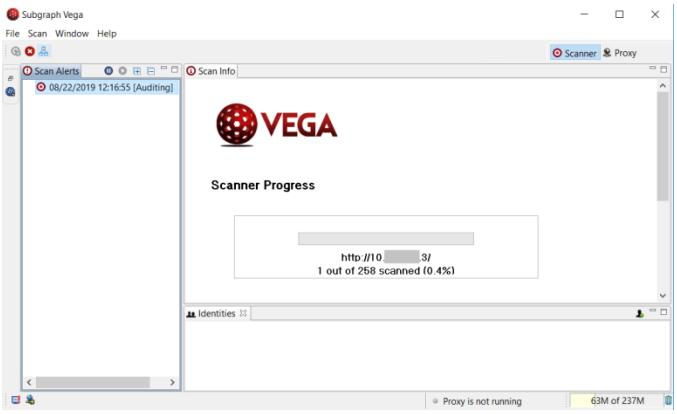

Fig. 7. OS Bash Injection Attack Attempt.

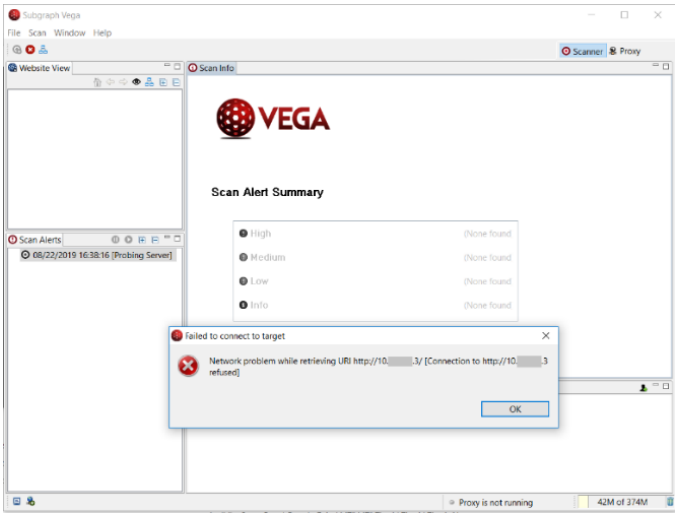

Fig. 8. Blocked Attacker Network Access by NAC.

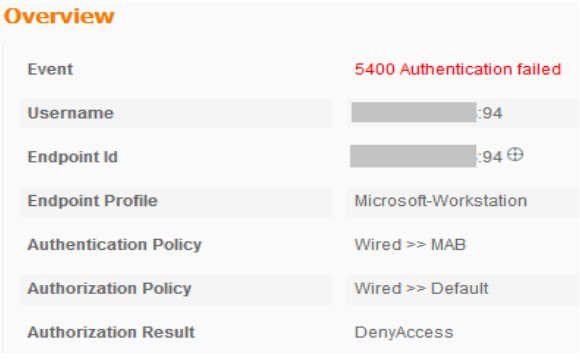

Fig. 9. Denied Network Access of Noncom Pliant user.

TABLE. II. RESULTS COMPARISON

No	User	Traffic	Target	Expectation	Result	
					NAC	**NAC & IPS (Proposed solution)**
1	Compliant	HTTP	Vulnerable OS	Allow	Allowed	**Allowed**
2	Compliant	SSH	Vulnerable OS	Allow	Allowed	**Allowed**
3	Compliant	SQL Injection Attack	Vulnerable OS	Block	Allowed	**Blocked**
4	Compliant	OS Bash Injection Attack	Vulnerable OS	Block	Allowed	**Blocked**
5	Noncompliant	HTTP	Vulnerable OS	Block	Blocked	**Blocked**

V. CONCLUSION AND FUTURE WORK

Based on the test results performed in this study, the proposed solution is that by integrating the NAC system with the IPS can mitigate attacks from internal users on internal networks and attacks from internal networks. That network security with the integration of the NAC systems with the IPS can be increased as compared to the use of the NAC alone. However, this study still has many limitations, particularly on the types of attacks tested. There are so many different types of attacks on the internet. Therefore, in the future it is recommended to increase the types of attacks carried out in similar tests and do more detail experiment to compare the application on the internal network with the application on the external network in order to achieve a more comprehensive result.

REFERENCES

[1] W. Bul'ajoul, A. James and M. Pannu, "Improving network intrusion detection system performance through quality of service configuration and parallel technology," Journal of Computer and System Sciences, vol. 81, no. 6, p. 981–999, 2015.

[2] W. Bul'ajoul, A. James and S. Shaikh, "A New Architecture for Network Intrusion," IEEE Access, vol. 7, pp. 18558-18573, 2019.

[3] H. A. Razzak, A. Karim, S. S. Handa and M. V. Ramana Murthy, "A methodical approach to implement intrusion detection system in hybrid network," International Journal of Engineering Science and Computing, vol. 7, no. 3, pp. 4817-4820, 2017.

[4] G. Ahmed, M. N. A. Khan and M. Shamraiz, "A linux-based IDPS," Computer Fraud & Security, pp. 13-18, 2015.

[5] [5] S. P. Anilbhai and C. Parekh, "Intrusion detection and prevention system for IoT," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 2, no. 6, pp. 771-776, 2017.

[6] S. Khadafi, B. D. Meilani and S. Arifin, "Sistem keamanan open cloud computing menggunakan ids (intrusion detection system) dan ips (intrusion prevention system)," Jurnal IPTEK, vol. 21, no. 2, pp. 67-76, 2017.

[7] F. Arsin, M. Yamin and L. Surimi, "Implementasi security system menggunakan metode IDPS (intrusion detection and prevention system) dengan layanan realtime notification," semanTIK, vol. 3, no. 2, pp. 39-48, 2017.

[8] A. Borkar, A. Donode and A. Kumari, "A survey on intrusion detection system (IDS) and internal intrusion detection and protection system (IIDPS)," in International Conference on Inventive Computing and Informatics, 2017.

[9] M. Warren, "Modern IP theft and the insider threat," Computer Fraud & Security, no. 6, pp. 5-10, 2015.

[10] F. Y. Leu, K. L. Tsai, Y. T. Hsiao and C. T. Yang, "An internal intrusion detection and protection system by using data mining and forensic techniques," IEEE Systems Journal, pp. 1-12, 2015.

[11] R. S. Silva and E. L. C. Macedo, "A cooperative approach for a global intrusion detection system for internet service providers," Cyber Security in Networking Conference, vol. 1, pp. 1-8, 2017.

[12] J. F. Matthews, "Challenges to implementing network access control," SANS Institute InfoSec Reading Room, p. 2, 2017.

[13] M. Roopesh, G. Reethika, B. V. Srinath and A. Sarumathi, "Network access control," International Journal on Computer Science and Engineering (IJCSE). Vol. 9, pp. 338-343, 2017.

[14] M. S. Inamdar and A. Tekeoglu, "Security analysis of open source network access control in virtual networks," International Conference on Advanced Information Networking and Applications Workshops, vol. 32, pp. 475-480, 2018.

[15] M. A. Muhammad and A. Ayesh, "A behaviour profiling based technique for network access control systems," International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 8, no. 1, pp. 23-30, 2019.

[16] A. Sood, "Network access control," Rivier Academic Journal, vol. 3, pp. 1-12, 2007.

[17] T. J. Dildy, "Network access control-has it evolved enough for enterprises?," ISACA Journal Vol. 4, pp. 1-5, 2016.

[18] K. O. Detken, M. Jahnke, C. Kleiner and M. Rohde, "Combining network access control (nac) and siem functionality based on open source," in IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Bucharest, 2017.

[19] R. R. Chaudhari and S. P. Patil, "Intrusion detection system: classification, techniques and datasets to implement," International Research Journal of Engineering and Technology, vol. 4, no. 2, pp. 1860-1866, 2017.

[20] V. Mahajan and S. K. Peddoju, "Deployment of intrusion detection system in cloud: a performance-based study," IEEE Computer Society, pp. 1103-1108, 2017.

[21] R. Jamar, A. Sogani, S. Mudgal, Y. Bhadra and P. Churi, "E-shield: detection and prevention of website," IEEE International Conference On Recent Trends in Electronics Information & Communication Technology, vol. 2, pp. 706-710, 2017.

[22] B. Y. Choi and D. G. Allison, "Intrusion prevention and detection in small to medium-sized enterprises," in SAIS, 2017.

[23] P. Rengaraju, V. R. Ramanan and C.-H. Lung, "Detection and prevention of DoS attacks in software-defined cloud networks," IEEE Conference on Dependable and Secure Computing, pp. 217-223, 2017.

[24] G. Duppa and N. Surantha, "Evaluation of network security based on next generation intrusion prevention system," Telkomnika, vol. 17, no. 1, pp. 39-48, 2019.