# CSOC

*By* Irfan Syamsuddin

WORD COUNT 3642
TIME SUBMITTED 01-JUL-2022 04:20PM
PAPER ID 87921073

# Evaluation of a Novel Intelligent Firewall Simulator for Dynamic Cyber Attack Lab

Irfan Syamsuddin(✉), Rini Nur, Meylanie Olivya, Irmawati, and Zawiah Saharuna

Center for Applied ICT Research (CAIR), Department of Computer and Networking Engineering, Politeknik Negeri Ujung Pandang, Makassar, Indonesia
{irfans,rini,meylanie,irmawati,zawiah}@poliupg.ac.id

**Abstract.** Firewall administration is an important topic in network security courses. However, most teaching aids of the topic commonly deal with static firewall analyses that does not adequately covers current dynamic and variety of cyber security attacks. This study presents our approach to introduce an intelligent firewall simulator to fill the gap. The simulator is based on iNetwork software and it has three different dynamic security attacks scenarios or modules. Each module is equipped with handbook or manual to aid student performs the simulation procedures. Evaluation of intelligent firewall simulator usage is performed by expert and student. Expert evaluation is focused on the content validity of the modules and its accompanying handbook, whilst student evaluation measures the perception of students after using the simulator. Finally, both evaluations show positive results that the content and manual of intelligent firewall modules are valid and also effective to improve student skills and understanding.

**Keywords:** Intelligent firewall · Simulation · Teaching module · Evaluation

## 1 Introduction

Vocational higher education such as polytechnics applies specific model of higher education which provides greater portion of hands on practices in comparison to theoretical concepts in the fields of science and technology. Hence it is commonly found that polytechnic students spend more time doing practical assignments than theoretical lectures in the classroom. As the result, vocational students have stronger problem solving abilities which equip them well to face most problems when they get job which is very much demanded by the industry. However, the challenges faced by higher education in developing countries are the ability of the institution to provide appropriate teaching facilities to students due to amongst other funding limitation. This impacts on the capability of instructor to provide adequate learning aids and supports to students.

Similar situation might be found at the Department of Computer and Networking Engineering (NCE) Department at State Polytechnic of Ujung Pandang (PNUP) where students deal with practicum-based assignments within 4 years of study period. One of


R. Silhavy (Ed.): CSOC 2020, AISC 1225, pp. 257–267, 2020.
https://doi.org/10.1007/978-3-030-51971-1_21

the big challenges in the process of teaching hands on practice course such as Computer Network Security (CNS) is the need for hardware to let the students practicing various practical exercises in a special laboratory. The provision of special laboratory with particular hardware, such as firewalls, routers and switches, requires very large cost, which is generally difficult to satisfy by higher education institutions due to limited budget allocation [1]. Moreover, for advanced topics such as CNS course, the designated laboratory must be strictly isolated from existing computer networks in campus while still have access to the Internet. This logical separation is urgent in order to block any possibilities of misuse by students during practical courses that could affect or even damage computer network infrastructure, partly or even entirely [2].

Considering the issues, several simulators software were introduced to enable students to perform practical assignments in CNS course without extra hardware installation in the laboratory. There are several simulator software that have been applied so far, such as Cisco Packet Tracer, GNS3, NS2 and iNetwork as reported in a working in progress paper [3]. We have developed a novel Intelligent Firewall Simulator (IFS) to fill the gap of unavailability of firewall simulator to intelligently deal with dynamics and various types of cyber attacks. The main purpose of current study is to evaluate the effectiveness of our approach. The evaluation is performed by considering expert and student views towards three main research questions as follows:

- How valid is the content of intelligent firewall simulator (IFS) modules with respect to the curriculum?
- How valid is the IFS manual for guiding the user?
- Does the use of IFS improve the understanding and skills of students?

The rest of this paper is structured as follows. Section 2 describes literature review, while the methodology and tools used to conduct the research are presented in Sect. 3. Then, results and discussion are given in Sect. 4. Finally, the study is summarized in the last section.

## 2 Literature Review

Using simulation tool in learning computer network security is considered beneficial from many aspects, such as design, implementation and evaluation. From design perspective, network simulations allow student to establish simple to complex network topology without extra cost and physical space. From implementation point of view, student could apply any scenarios easily and they are fully under controlled. Then, in terms of evaluation, it is easier to perform evaluation on simulator environments rather than in real physical ones. As a results, simulation approaches have been gaining popularity in recent decades [2, 3].

The use of computer network simulator has been regarded as an appropriate answer to deal with limited physical laboratory facilities. Although, to a certain extent, computer network simulator could not fully present ideal look and feel of the actual network behaviour. In case of a firewall, basic concept of how firewall is configured or how it works in ruling the network flow as well as data flow analysis behind the work of the firewall can be learned by using simulator software [4]. Pastor et al. [4] argue that

implementation of computer network software in which several firewalls combined has brought many benefits in enhancing the learning process, and significantly reduces cost of laboratory development in case of open source software as exemplified in recent studies [3, 5].

Another approach to enable firewall simulation was described by Yan [6] using cloud computing technology. However, the approach requires the existence of a physical network to the cloud that not all institutions could provide. Hajdarevic, et al. [7] discuss the use of GNS3 simulator in assessing firewall rules through a dedicated training of ethical hacker. They assert that GNS3 offers a flexible way to learn network security particularly firewall mostly in Linux environment [7]. Web based firewall was also proposed by Trabelsi and Mustafa [8]. This is a unique approach in which user needs only a browser to run the application, create topology, connecting all devices, define firewall rules and analyze the simulation results. Similar approach is presented by Losilla [9] with assessment tool in wireless network.

In addition, Opnet based simulation for firewall was reported by Ameen and Nourildean [10]. The authors apply a cloud topology to investigate firewall impact on the network over Opnet simulator. Similarly, Al-Hilfi et al. [11] also employed Opnet to assess firewall functions in terms of wireless LAN security. Both papers argue that Opnet is a powerful tool in tackling firewall simulations. Likewise, Cisco's packet tracer is considered as the most widely used simulator in learning firewall and network security topics [12]. It has been used in teaching computer security at undergraduate level by Airi and Anderson [13]. Also, a study by Dengping et al. [14] shows that the simulator is appropriate simulator for computer network management course. More recently, Zhang et al. [15] report their positive results in using simulator for teaching information security course. However, the software is vendor oriented for Cisco products.

In [16], a novel network simulator called iNetwork was introduced for the first time. It is a very lightweight application that does not need heavy hardware requirements. This Java-based simulator could be run on various versions of Windows machines without the installation process just by copying the given folder. Besides, the GUI design is very interactive and easy to use even by beginners. The most important feature of iNetwork is its' built in tutorial covering wide range computer network topics including firewall [16, 17].

Moreover, iNetwork offers flexibility and portability in firewall simulation by providing two options to perform firewall simulation and testing. The first option is by using the existing iNetwork Simulator utilities such as ping command through windows command line. Secondly, the test can be done via packets GUI for managing ICMP, TCP or UDP packets data sending. In addition, the simulation results are viewed using the existing Activity Log interface [17].

Among the aforementioned simulation tools, most of them cover firewall simulation in static way of firewall administration. In other words, they not adequately cover current dynamic and variety of cyber security attacks. This is why we need to introduce an intelligent firewall simulator to fill the gap. Based on our experiences, iNetwork simulator has the capacity to apply intelligent firewall simulation. Therefore, we extend the simulator by developing a novel simulator called Intelligent Firewall Simulator (IFS) that offers capabilities to fill the gap found in current literature. The IFS consist of

three scenarios called modules to illustrate different cyber-attacks and how an intelligent firewall deals with them. Each module is accompanied by tutorial to guide student performing hands on lab activities.

## 3 Tools and Method

Main tool used in the study is iNetwork simulator which has various networking simulation topics from peer to peer networking to firewall and wireless simulations [16, 17]. Its rich features with low computing requirements makes it fit to our curriculum and laboratory needs. Unfortunately, iNetwork only provides simple and static firewall simulation which could not support the dynamic one. Therefore, Intelligent Firewall Simulator (IFS) is developed as an extension of iNetwork simulator to fill the gap of dynamic firewall simulation.

The main feature of IFS is its ability to simulate advanced dynamic firewall which is adaptive to different attacks scenarios. Such ability is known as intelligent firewall that can be simulated o deal with recent dynamic cyber attacks should be well understood by students during hands on practical lab session.

Figure 1 shows the main interface of Intelligent Firewall Simulator (IFS) running over iNetwork simulator. IFS's core function is to apply log analysis from previous blocked packets and sources in order to understand whether there were current access in an attack or not. This feature is not available in standard iNetwork simulations. It works by mining log data (not saved by iNetwork) and use them as input which firewall can reference when making decision. Therefore IFS showcases novel simulation processes on the dynamic prevention of various forms of attacks. We structure the IFS simulation with three scenarios represented as beginner, intermediate and advanced modules with increasing filtering rule complexity, respectively. In order to help students practicing the lab independently each module has manual or lab guide which is clear enough to assist them doing the simulation and understand how intelligent firewall works effectively.

The beginner module has 3 rules that might be applied dynamically by firewall administration which expected to be finished within 30 min. The next one called intermediate module has 6 rules applied to the intelligent firewall simulator. The last module is a bit more complex with 10 rules which requires approximately 90 min for students to practice and evaluate it (see Table 1).

The following figures show the network structures of three modules of IFS. For beginner and intermediate modules, the rules are similar that it should be done individually. Once students finishing all tasks as mentioned in lab manual, they should submit written reports describing their lab activity results found in both modules (Fig. 2).

While in the advanced module (Fig. 4), students work in groups instead individual. At the end of lab activity, every group make presentation on their simulation process and also defend their findings and opinions during the question and answer session (Fig. 3).

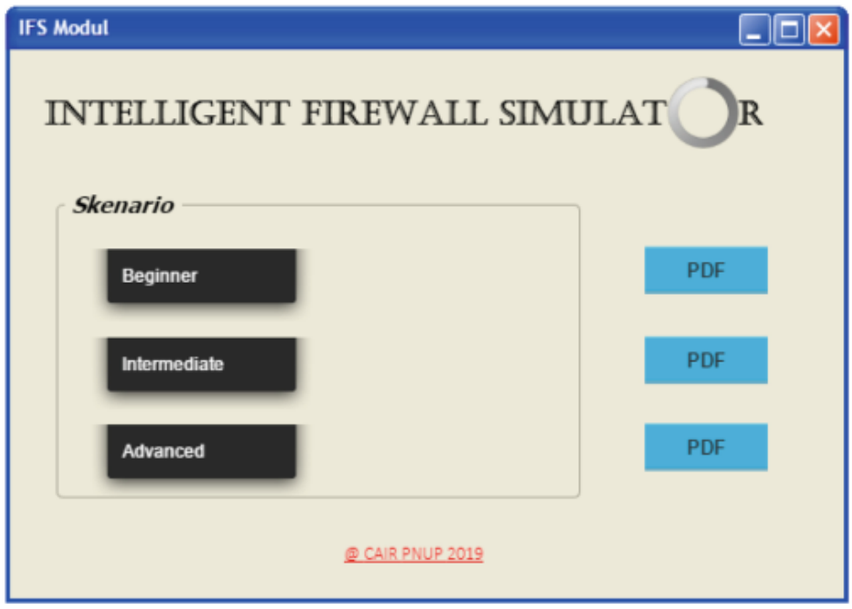


**Fig. 1.** Interface of Intelligent Firewall Simulator

**Table 1.** Firewall simulation modules.

| Heading level | Number of rules | Network components | Expected time to finish |
|---|---|---|---|
| Beginner | 3 | PC (4), Switches (1) | 30 min |
| Intermediate | 6 | PC (3), Switches (2), Router (2), Web Server (1) | 60 min |
| Advanced | 19 | PC (3), WirelessPC (2), Access Point (1), Switches (3), Router (3), Web Server (1), DNS Server (2), Mail Server (2) | 90 min 10 point, bold |

In order to deal with three research questions aforementioned in previous section, three surveys were constructed based on previous related studies. Participants of the survey are classified into expert and student groups.

The first survey was developed in accordance with studies by Muharram, et al. [18] and Syamsuddin [19]. It was a content validity survey which was aimed at evaluating the validity of IFS modules which consists of five questions such as connection with the topics, educational aspects, tool usability, practicability of module and learning module development value. This survey was administered to the expert group.

The second survey, which was also given to the expert group, was structured according to study in [19]. Its aim was to evaluate validity of accompanying tutorial or module from four aspects namely, content, language, layout and learning.

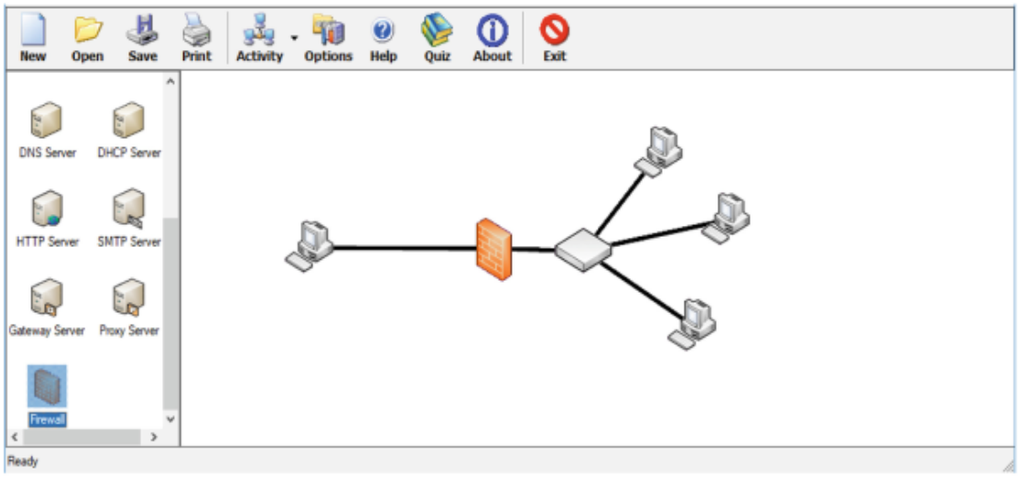


**Fig. 2.** The beginner module of IFS

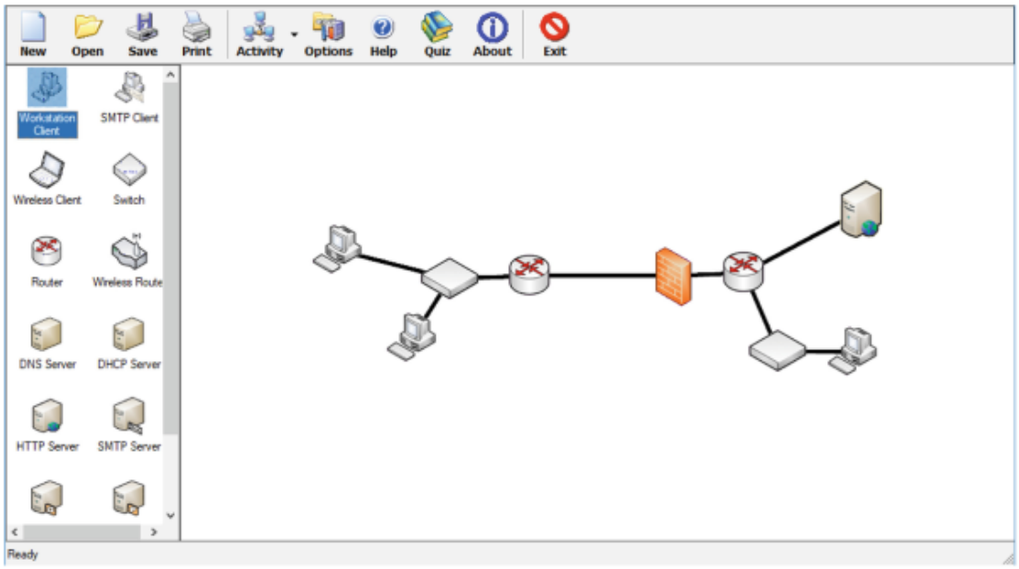


**Fig. 3.** The intermediate module of IFS.

The third survey was given to students. The survey was based on Muharram, et al. [18] intended to obtain users' perception after using IFS modules. Through the last survey, effectiveness of the modules in enhancing student knowledge and skills in related course might be measured.

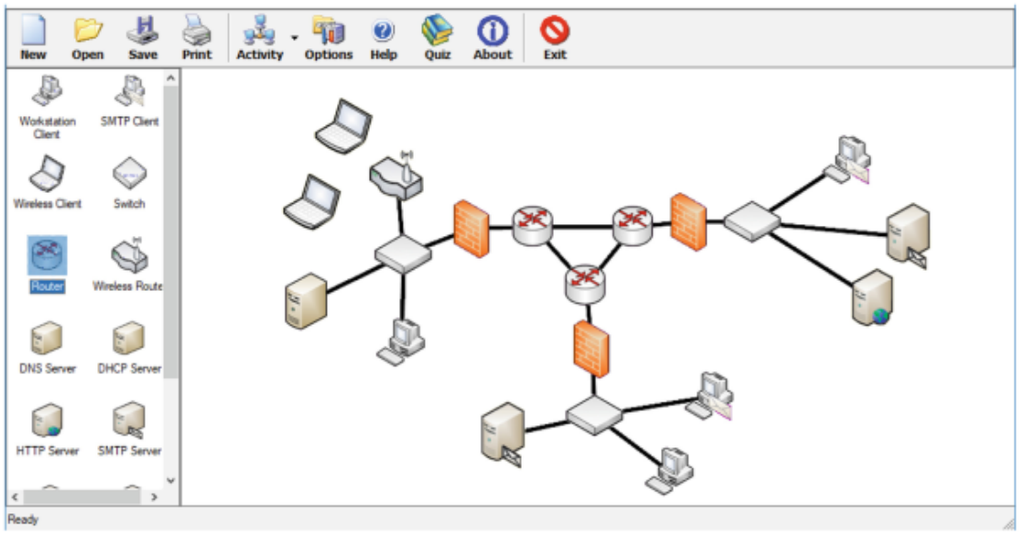


**Fig. 4.** The advanced module of IFS

## 4 Results and Discussion

Five experts involved in the first survey on content validity which consists of five questions. The question uses likert scales, ranging from 1 (represents the worst) to 5 (represents the best). The process is as follows. After having all responses from experts then the process is continued by calculating the mean score of each criterion. Finally, it is finalized by calculating validity score (VS) which is actually the mean value of all five criteria.

The mean score of the five criteria are 3.7, 3.96, 3.76, 4.08 and 3.54 respectively. The highest score goes to practicability of the module, while the lowest score goes to learning development value. In short, these yield validity score of 3.8 for the content validity. Based on this value, it is clearly indicated that the experts agree to acknowledge that the content of iNetwork based firewall simulation modules are acceptable and valid (Table 2 and Fig. 5).

**Table 2.** First survey on content validity.

| No. | Validity criteria | E1 | E2 | E3 | E4 | E5 | M |
|---|---|---|---|---|---|---|---|
| 1 | Connection with the topics | 3.9 | 3.7 | 3.5 | 3.8 | 3.6 | 3.70 |
| 2 | Educational aspects | 3.8 | 4.5 | 4.5 | 3.4 | 3.6 | 3.96 |
| 3 | Tool usability | 3.6 | 3.8 | 4 | 3.8 | 3.6 | 3.76 |
| 4 | Practicability of module | 4 | 3.8 | 4.6 | 3.8 | 4.2 | 4.08 |
| 5 | Learning module development value | 3.2 | 3.4 | 3.9 | 3.8 | 3.4 | 3.54 |

Validity Score (VS) 3.8

The second evaluation is to measure validity of the manual or handbook accompanying each module. The same experts are involved in this survey which covers four aspects, namely content, language, layout and learning. Similar to previous survey,

each question has likert scale from 1 (represents worst) to 5 (represents best) as alternative choices by the respondents. The result of the second survey is presented in the following table (Fig. 6).

Likewise, after all experts select their preferences on each question, then we calculate the mean score of each question. It is revealed that the mean scores are 3.92, 3.78, 4.02 and 3.88 respectively. The highest score goes to layout while the lowest one is language. These yield validity score of 3.9 for the handbook. The findings show that all experts agree on the validity of the handbook accompanying the three modules of IFS since they provide clear and easy to understand practical guideline for student (Table 3).

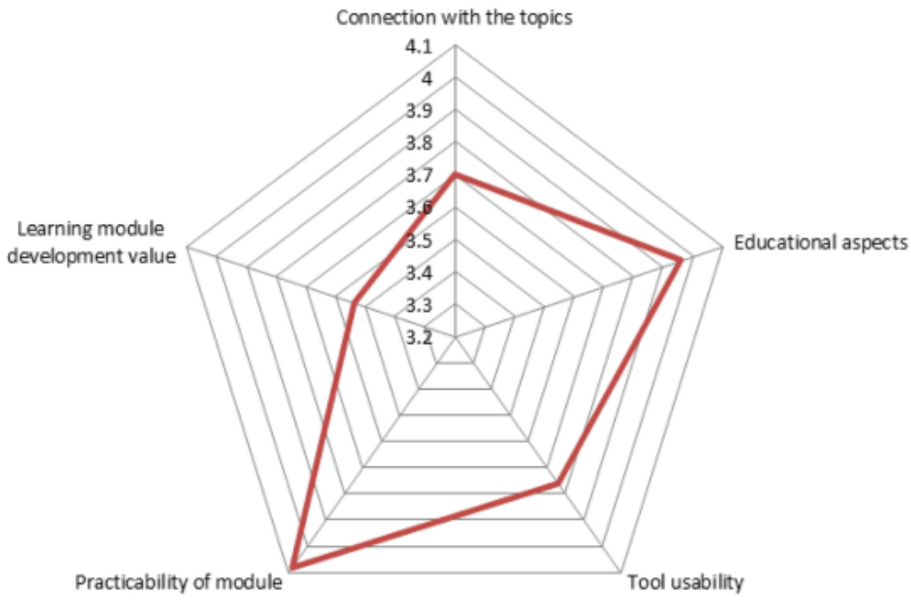


**Fig. 5.** Result of content validity.

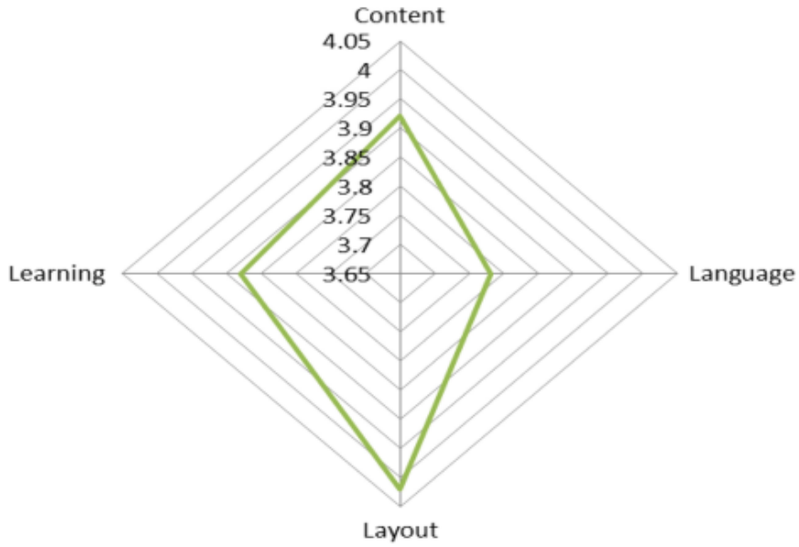


**Fig. 6.** Result of handbook validity.

**Table 3.** Second survey on handbook validity.

| No. | Validity criteria | E1 | E2 | E3 | E4 | E5 | M |
|---|---|---|---|---|---|---|---|
| 1 | Content | 3.6 | 3.9 | 4.4 | 4.1 | 3.6 | 3.92 |
| 2 | Language | 3.4 | 4 | 4.1 | 4.1 | 3.3 | 3.78 |
| 3 | Layout | 3.8 | 4 | 4.4 | 4.2 | 3.7 | 4.02 |
| 4 | Learning | 3.8 | 3.8 | 4.3 | 4 | 3.5 | 3.88 |

Validity Score (VS) 3.9

The last evaluation was carried out with the purpose of obtaining students' perceptions in using IFS. The survey also uses a typical likert scale with the same options of Strongly Disagree (SD), Disagree (D), Neutral (N), Agree (A), and Strongly Agree (SA) and assign 1, 2, 3, 4, 5 values respectively. All students participated in this voluntary survey and the results are shown in the following figure (Fig. 7).

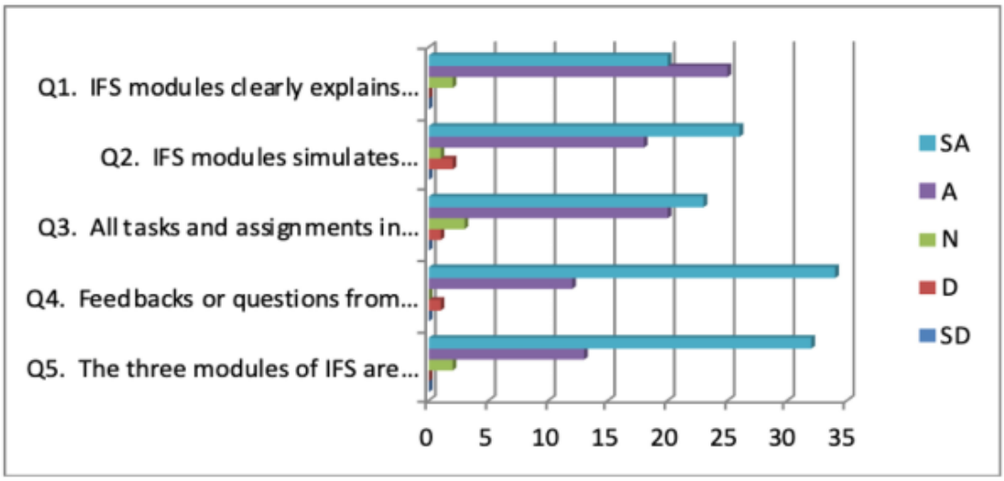


**Fig. 7.** Result of the last survey.

In the first question which addresses clarity of the module to explain the principles firewall concept in network security, 25 students agree and 20 of them strongly agree, while only 2 students are neutral. In the second question concerning their understanding through intelligent firewall operations, 26 students strongly agree and 18 others agree while two students do not agree and one of them neutral. In terms of assignments of the third question, 23 students strongly agree and 20 of them agree, while a student disagree and three of them neutral. For the fourth question regarding students' feedback and questions, 34 students strongly agree and 12 others agree while only one disagrees. Then in terms of the final question, 32 students strongly agree and 13 of them agree while two students neutral.

## 5 Conclusion

A novel Intelligent Firewall Simulator (IFS), simulation processes on the dynamic prevention of various forms of attacks described in this paper. IFS consists of beginner, intermediate and advanced modules to facilitate effective students learning by following the given step-by-step lab manuals. The implementation of IFS is evaluated from expert and student point of views.

In short, experts agree that both content and handbook are valid and acceptable as seen by total validity score of 3.9 for content and total validity score of 3.8 out of 5. Similarly, the students in the last survey conclude that the use IFS in learning is perceived useful to enhance their understanding.

It is expected for future research to adopt gamification approaches in order to enrich IFS learning experience and to improve student engagements. Another promising future research direction is to apply problem based learning with real network security scenarios.

## References

1. Van Leeuwen, B., Eldridge, J., Urias, V.: Cyber analysis emulation platform for wireless communication network protocols. In: International Carnahan Conference on Security Technology (ICCST), pp. 1–6 (2017)
2. Gaffer, S.M., Alghazzawi, D.M.: Using virtual security lab in teaching cryptography. Int. J. Modern Educ. Comput. Sci. **1**, 26–32 (2012)
3. Syamsuddin, I.: VILARITY: a virtual lab for teaching computer security. TEM J. Tech. Educ. Manage. **8**(3), 125–130 (2019)
4. Pastor, V., Díaz,G., Castro, M.: State-of-the-art simulation systems for information security education, training and awareness. In: Education Engineering (EDUCON), pp. 1907–1916 (2010)
5. Montero, Á. M., Manzano, D. R.: Design and deployment of hands-on network lab experiments for computer science engineers. Int. J. Eng. Educ. **33**(2), 142–149 (2017)
6. Yan, C.: Build a laboratory cloud for computer network education. In: Proceedings of the 6th International Conference on Computer Science & Education (ICCSE 2011), pp. 1013–1018 (2011)
7. Hajdarevic, K., Kozic, A., Avdagic, I., Masetic, Z., Dogru, N.: Training network managers in ethical hacking techniques to manage resource starvation attacks using GNS3 simulator. In: XXVI International Conference on Information, Communication and Automation Technologies (ICAT), pp. 1–6 (2017)
8. Trabelsi, Z., Mustafa, U.: A web-based firewall simulator tool for information security education. In: Proceedings of the Sixteenth Australasian Computing Education Conference, vol. 148, pp. 83–90 (2014)
9. Losilla, F.: A web-based design and assessment tool for educational wireless networking projects. Comput. Appl. Eng. Educ. **25**(6), 992–1000 (2017)
10. Ameen, S.Y., Nourildean, S.W.: Firewall and VPN investigation on cloud computing performance. Int. J. Comput. Sci. Eng. Surv. **5**(2), 15–21 (2014)
11. Al-Hilfi, H.M.T., Salih, B.A., Marghescu, I.: Design of secured WLAN by using packet filtering firewall. In: International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1857–1862 (2017)

12. Javid, S.R.: Role of packet tracer in learning computer networks. Int. J. Adv. Res. Comput. Commun. Eng. **3**(5), 6508–6511 (2014)
13. Airi, P., Anderson, P.K.: Cisco packet tracer as a teaching and learning tool for computer networks. DWU Res. J. **26**, 67–72 (2017)
14. Dengping, T., Yanqin, Z., Zhe, Y., Guoping, C., Guangdi, X.: Design of firewall experiment based on computer network management simulation platform. Exp. Tech. Manage. **4**, 39–47 (2015)
15. Zhang, T., Yin, M., Yang, Y.: An experiment teaching mode for an Introduction to Information Security course. World Trans. Eng. Tech. Educ. **12**(4), 725–728 (2014)
16. Sandrasegaran, K., Trieu, M.: iNetwork: an interactive learning tool for communication networks. In: Tools for Teaching Computer Networking and Hardware Concepts, pp. 39–61 (2006)
17. Ye, M., Sandrasegaran, K.: Teaching about firewall concepts using the iNetwork Simulator. In: 7th International Conference on Information Technology Based Higher Education and Training, ITHET 2006, pp. 889–892 (2006)
18. Muharram, Adnan, Sudding: The development of an enzyme catalase kit for engineering students at technical vocational schools. Global J. Eng. Educ. **19**(2), 168–172 (2017)
19. Syamsuddin, I.: Evaluation of NgeXTEA - a cryptography learning module. Global J. Eng. Educ. **20**(3), 196–200 (2018)

# CSOC

ORIGINALITY REPORT

4%
SIMILARITY INDEX

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | d.researchbib.com<br>Internet | 45 words — 1% |
| 2 | wiete.com.au<br>Internet | 22 words — 1% |
| 3 | bearworks.missouristate.edu<br>Internet | 18 words — 1% |
| 4 | www.temjournal.com<br>Internet | 18 words — 1% |
| 5 | www.hindawi.com<br>Internet | 14 words — < 1% |
| 6 | cfsites1.uts.edu.au<br>Internet | 10 words — < 1% |

| | | | |
|---|---|---|---|
| EXCLUDE QUOTES | ON | EXCLUDE SOURCES | < 10 WORDS |
| EXCLUDE BIBLIOGRAPHY | ON | EXCLUDE MATCHES | < 9 WORDS |