MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS (2023) 6 (1) 10-20

DOI: *https://doi.org/10.37231/myjcam.2023.6.1.85*

Article: Received 21.11.2022; Accepted 11.02.2023; Published 31.03.2023

TOWARDS SECURE LOCAL AREA NETWORK (LAN) USING OPNSENSE FIREWALL

Che Ku Nur Syakirul Aiman Che Ku Mohamad Rafee✉, Nor Surayati Mohamad Usop

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut Campus, Malaysia
✉060057@putra.unisza.edu.my

Abstract: OPNsense is an open-source firewall and routing platform that is based on the FreeBSD operating system. It is designed to be easy-to-use and easy-to-build, making it a suitable solution for both small and large organizations. OPNsense offers a wide range of features that are comparable to those found in expensive commercial firewalls, and in many cases, it even offers more. The platform includes a web interface and a powerful package manager, which allows for easy customization and management of the firewall. OPNsense is a fork of the popular pfSense firewall and is known for its high level of security, stability, and performance. It is an ideal solution for organizations looking for a cost-effective, flexible, and secure firewall solution. The number of users today is growing along with networking technology. To transport data through a network, each user can communicate with one another. However, when the network expands, a network administrator must keep an eye on Flows of traffic or bandwidth that pass via networks. Some users who access the Internet erratically could lead to a bottleneck situation. The major goal is to create a evaluate effectiveness of the firewall also monitoring and securing network.

Keywords: OPNsense, Graphical User Interface, Local Area Network, Intrusion Detection System, Intrusion Prevention System.

1. INTRODUCTION

OPNsense is a FreeBSD-based open-source firewall and routing framework. It began in 2014 as a fork of the popular pfSense firewall solution, with the purpose of delivering a more modern, secure, and adaptable firewall solution [1]. OPNSense is a comprehensive firewall and routing system that prioritizes security, dependability, and usability. Its user-friendly web interface makes managing firewall rules, VPNs, and other security features simple, while complex capabilities like intrusion detection and prevention, URL filtering, and traffic shaping make it suited for usage in both small and big enterprise contexts. However, the growing threat of Distributed Denial of Service (DDoS) Attacks presents a serious challenge to the firewalls, which can be overpowered by high-volume DDoS attacks. This can have serious repercussions, including identity theft, financial fraud, and other cybercrimes. Decreasing the performance of the system and perhaps permitting unauthorized traffic. Along with the firewall, using specialized DDoS mitigation tools or services can assist reduce such attacks.

Despite significant research efforts in more protect the network from such attacks from happening, there remains a gap in effectively mitigating the risk of Distributed Denial of Service (DDoS) attacks. While existing approaches focus on packet filtering and stateful inspection, they often do not sufficiently address the vulnerability of the firewall. Attackers can exploit the firewall through Zero-day exploits, which are vulnerabilities unknown to the security community, can bypass firewall defences as there may not be corresponding signatures or rules to detect them [2]. To address this gap and enhance network security of the firewall, this paper proposes a novel approach that leverages the intrusion detection and prevention technique in combination with the threat Intelligence Integration system. These systems monitor network traffic for suspicious patterns or known attack signatures. They can alert administrators or take proactive measures, such as blocking or dropping malicious traffic. Thereby increasing the complexity for attackers attempting to compromise the system. This approach complements the Threat Intelligence Integration, so that OPNsense firewalls can leverage threat intelligence feeds to stay updated with the latest information about emerging threats, malicious IP addresses, or known attack patterns. By incorporating threat intelligence, firewalls can proactively block or flag traffic from known malicious sources [3][4].

The primary objective of this research is to mitigate the risk of application layer attacks on network of the firewall by implementing the User and Application Control technique and Deep Packet Inspection. By inspects the payload and performs in-depth analysis, allowing the firewall to detect and block malicious content or activities that may be hidden within the packet payload., the system aims to thwart their efforts to hack the network and intruders.

In this paper, we will first provide an overview of the background of OPNsense firewall configuration, highlighting the vulnerabilities associated with attacks on the network. We will then present a detailed analysis of the Application Control technique and Deep Packet Inspection technique, explaining their principles and evaluating their effectiveness in preventing unauthorized access. Additionally, we will describe the implementation of the configure OPNsense and use its features in an effort to safeguard the OSI model's network and transport layer, along with the strategies employed to engage and prevent attackers. Important to recognize these limitations and complement OPNsense firewall protection with additional security measures such as intrusion detection systems, strong access controls, regular vulnerability assessments, user education, and monitoring mechanisms to mitigate the risks posed by these disadvantages.

2. RELATED WORKS

2.1 Cross-VM Cache Timing Attacks on Virtualized Network Functions

The author use of firewalls as a network appliance plays a crucial role in providing protection to the internal networks by filtering incoming adversarial packets [1]. Firewall policy, which is represented as a collection of filtering rules in the form of an Access Control List (ACL), determines the packets that are allowed to pass through. Each rule specifies the characteristics of the matched packets, such as the source and destination address and port numbers, and the corresponding actions, such as accept, drop, or reject. While firewall policy reconnaissance is a scanning technique that aims to gather information on the filtering rules of the target firewall in preparation for network intrusion. The reconnaissance is typically performed by observing the response packets to specially crafted probe packets. In recent research, a new reconnaissance technique has been proposed for co-located attackers that involves inferring the filtering rules by analyzing the cache behavior on a host in response to probe packets [2]. Many virtualized firewall products, such as VyOS, IPFire, OPNSense, and Smoothwall, are built on Linux kernels and utilize iptables, a kernel component, to provide the packet filtering functionality [4].

2.2 Engaging Students with Personalized and Remotely Orchestrated Cybersecurity Training Exercises

In this paper, the authors present a solution for network isolation and monitoring in a shared computing environment. To ensure the security and integrity of vulnerable software, strict network isolation measures are implemented through the use of physical hosts connected to a manageable switch, which has dedicated virtual local area networks (VLANs) configured. The management VLAN is used for interconnectivity between hosts and the bastion virtual machine, while the instantiated virtual machines used by students are placed in the remaining VLANs. To provide internet access, an OPNSense firewall appliance is utilized, chosen for its application programming interface (API) that allows for programmatic management. This solution allows for strict monitoring and limited internet access for vulnerable machines, making the scenario more realistic through the use of granular firewall rules [5].

2.2.1 Test-beds and guidelines for securing IoT products and for secure set-up production environments

The author of [6] the installation and evaluation of open-source security appliances, specifically IPFire and OPNsense, is presented. The objective of the study was to examine the features, usability, and reliability of these open-source firewalls, and to compare their performance to that of commercial firewalls. The theoretical background of firewalls and the protocols utilized by these security systems is also discussed. The hardware used in the testing process is described, along with the methodology and test environment. The results of the evaluation are analyzed and compared to provide a comprehensive understanding of the capabilities and limitations of open-source firewalls. The future prospects of these security systems are also briefly explored.

2.3 User and Application Control Technique

A firewall approach called User and Application Control enables administrators to impose rules based on user identities and certain apps. Here's how it functions. User-based Management Firewalls can link network traffic to particular user identities and authenticate users depending on their credentials, such as usernames and passwords. Administrators are now able to specify firewall limits and rules based on user or group roles. For instance, while restricting others, some individuals or user groups may be given higher privileges or access to particular resources. Firewalls can recognise and categorise network traffic based on the applications or protocols being used. This is known as application-based control. The firewall can identify the exact application or service involved with the traffic by looking at packet headers or payloads. In order to provide precise control over network access, administrators can then set policies to allow or deny traffic depending on the recognized apps. User and Application Control contributes to the enforcement of security policies that are customized to particular users and apps, lowering the attack surface and improving overall security posture [7].

2.4 Distributed Denial of Service (DDoS)

The attacks known as DDoS (Distributed Denial of Service) can be exceedingly challenging for firewalls to handle. Here are a few DDoS attacks on firewall mitigation techniques. Resource Depletion DDoS assaults flood network resources, such firewalls, with a lot of malicious traffic. If the amount of incoming traffic exceeds the processing capacity of firewalls, they may become overloaded and unable to handle legitimate traffic. In addition to a firewall, specialised DDoS mitigation tools and services can help decrease the effects of DDoS attacks. These solutions may employ a range of techniques, such as traffic profiling, rate limitation, traffic diversion, or specialised hardware, to detect and stop DDoS attacks before they reach the firewall.

This paper analyses the exploitable vulnerabilities in OPNsense firewall administrators and assesses the effects of Distributed Denial of Service (DDoS) on them [8]. The researchers use comprehensive testing and analysis to show that distributed denial of service (DDoS) poses a serious threat to the network because attackers can attempt to overwhelm network resources, such as firewalls, by flooding them with a large volume of malicious traffic. Due to their limited processing power, firewalls may become overloaded and unable to handle lawful traffic if the volume of incoming traffic exceeds their capability. Methodology is a systematic way that solve the research problem by applying technique, algorithm or method. It comprises theoretical analysis of methods and principles associated with a branch of knowledge.

Methodology also defines as principles, rules or procedure that use for developing a project or system. According to the project, methodology that shows in this chapter are flowchart and framework. In order to overcome problem stated in 1.2, this methodology builds referring to the three main objectives stated in 1.3. First, to study existing LAN infrastructure, second to design the simulation and lastly, to implement the simulation. This project will be focused on network monitoring.

Based to the project, Project Management Establish the goals, needs, and scope of the project in detail. Research and acquainting Oneself Study the OPNsense manual and become comfortable with the capabilities and online interface. System Configuration and Setup Install and set up OPNsense on a virtual machine or dedicated hardware. Implementation of Features Utilising the OPNsense plugins and modules at your disposal, identify desired features and implement them. Validation and Testing Make a test plan, run extensive testing, and confirm the features that were integrated. Assessment and Results Measure performance gains and the usefulness of the enhancements. Presentation of Documents Make thorough documentation and a presentation that summarises the project.

3. METHODOLOGY

A methodological approach to research problem solving employs a methodology, algorithm, or procedure. It includes a theoretical investigation of the practices and tenets related to a field of knowledge. Principles, guidelines, or procedures used in the development of a project or system are also referred to as methodologies. The project's flowchart and framework are the technique shown in this chapter. This methodology is built around the three primary goals listed in 1.3 in order to solve the challenge mentioned in 1.2. First, analyses the current LAN infrastructure, then create the simulation, and finally, put the simulation into practice. Network monitoring will be the main emphasis of this project.

Project Management is based on the project. Establish the project's objectives, requirements, and scope in great detail. research and familiarization Oneself Learn the capabilities and web interface by

reading the OPNsense documentation. Setting up and configuring the system Install and configure OPNsense on a dedicated piece of hardware or a virtual machine. the application of features Determine desired features and implement them using the OPNsense plugins and modules at your disposal. Testing and Validation Create a test strategy, conduct thorough testing, and validate the features that were incorporated. Results of assessment Evaluate improvements' utility and performance increases. Documentation Display Make thorough records and an overview presentation for the project.

4. IMPLEMENTATION

4.2.1 Installation of VMware Workstation 17 Pro

The base operating system for running OPNsense for the simulation firewall will be conduted with VMware Workstation 17 Pro version 17.0.0 build-20800274 . The following instructions will walkthrough the installation of VMware Workstation 17 Pro.Implementation and result are two of the most crucial steps in this project for simulating network setup. Before a project may be fully exploited, this step must be completed. The step-by-step setups and installation will be extensively detailed in this chapter to achieve the project's goal. The VMware operating system is specially utilized in this implementation and testing phased.

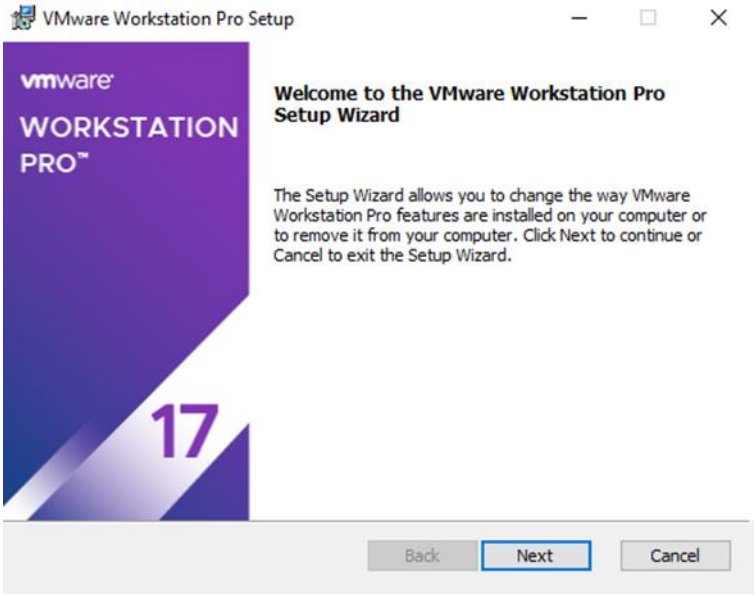

Figure 1: Installation of VMware Workstation 17 Pro

Figure 1 depicts the second stage of installing VMware Workstation 17 Pro to dual boot with Windows 10.

4.2.2 Installation and configuration of OPNsense

This section describes how to install and configure OPNsense in VMware Workstation 17 Pro. The first step is to get OPNsense Iso file by following the link and downloading the folder OPNsense-22.7-OpenSSL-dvd-amd64.iso.

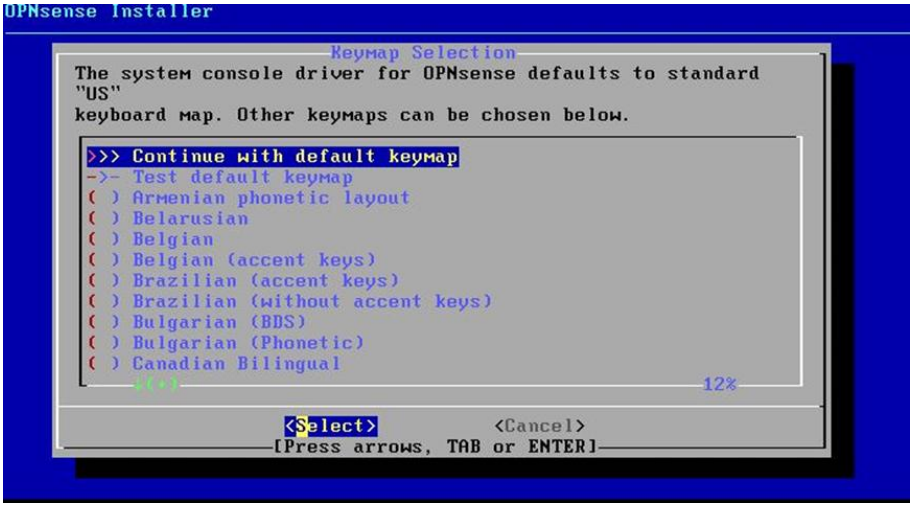

Figure 2 The OPNsense Installer

OPNsense should be installed and running on your system as in Figure 2.

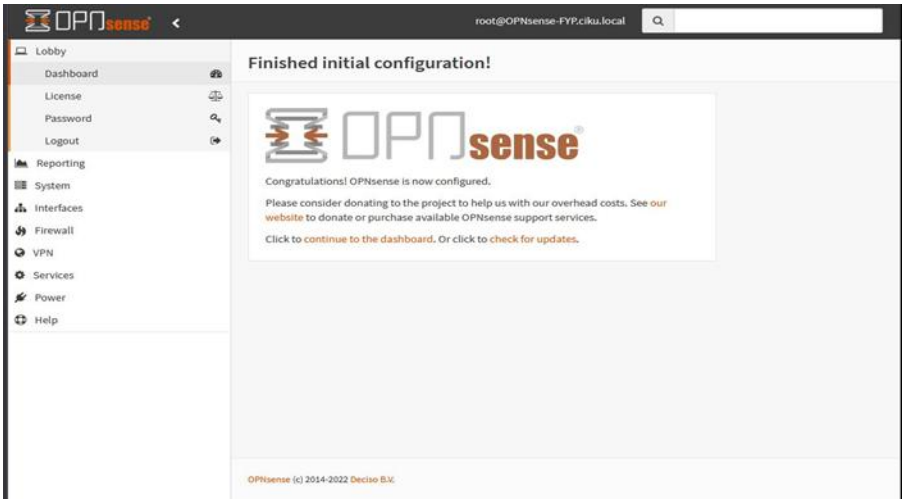

Figure 3 OPNsense Web Interface

This includes setting up network interfaces, configuring firewall rules, and configuring additional services as shown in Figure 3.

4.2.3 Implementation of ZenArmor in OPNsense firewall.

The Sunny Valley Networks vendor repository plugin must first be installed before ZenArmor can be installed. Visit the page for System, Firmware, and Plugins. To install the plugin, click on the "+" sign next to os-sunnyvalley. The ZenArmor plugin should be visible in the list of plugins as os-sensei once the vendor plugin has been installed. You might need to reload the "Plugins" page if the ZenArmor plugin is not visible. To add the plugin, click the "+" sign next to os-sensei.

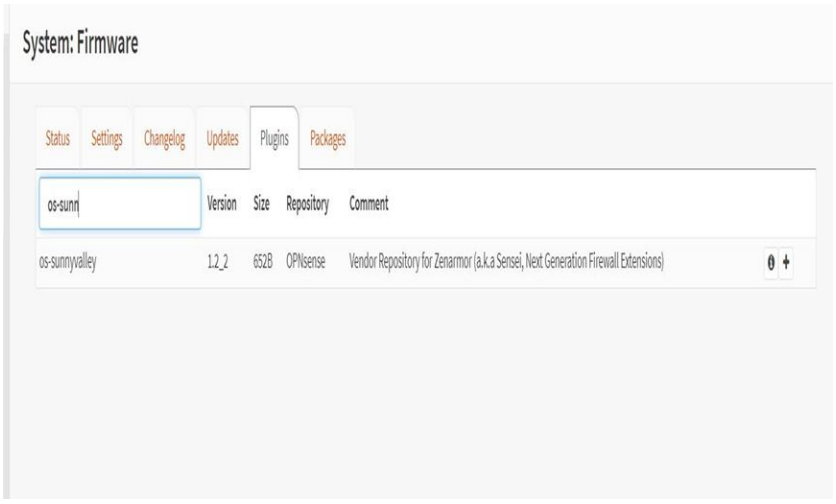

Figure 4 Initial Configuration Wizard of ZenArmor

After installing ZenArmor, you should see the ZenArmor menu in the left sidebar of the OPNsense web interface as shown in Figure 4.

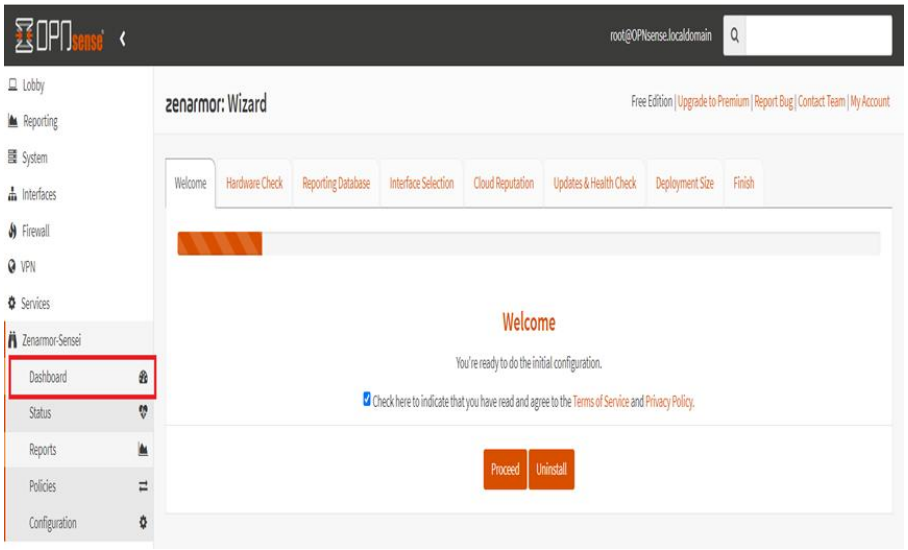

Figure 5 ZenArmor Welcome Page After Installation

Figure 5 shows that the package will be accessible on the OPNsense web interface once the installation is complete.

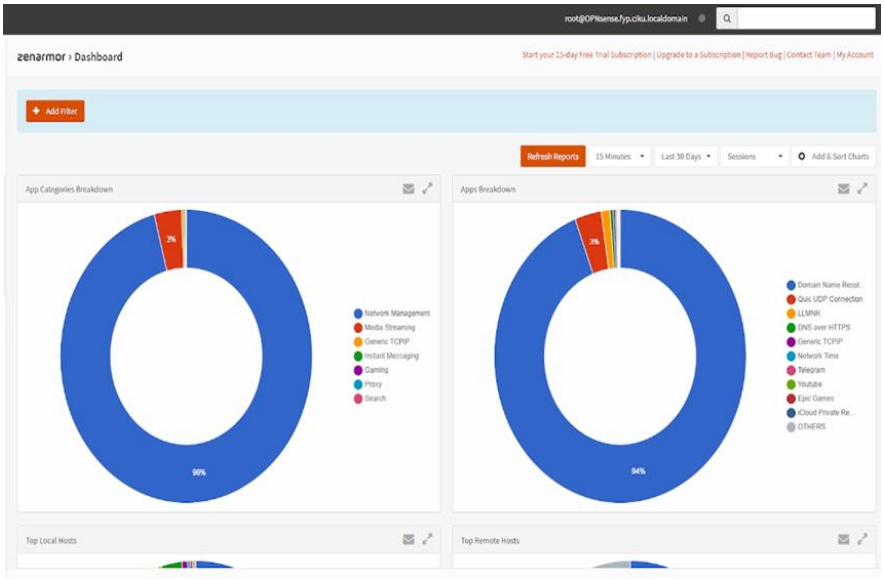

Figure 6 Reporting showcase with ZenArmor

Figure 6 shows tremendously rich reporting capabilities of ZenArmor allow users to both view the entire network activity from a high viewpoint and drill down to specifics by selecting any chart item.

Figure 7 Category blocking with ZenArmor

Figure 7 shows how blocking a category or an application, user of ZenArmor can restrict certain applications as well as an entire category of applications.

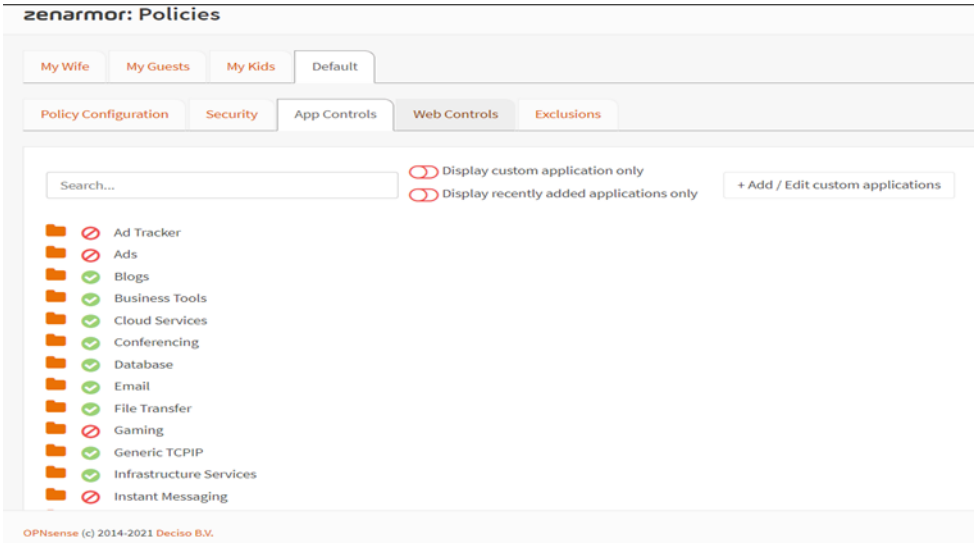

Figure 8 Content Blocking with ZenArmor

Figure 8 shows how blocking all content in a category (excludes Ad Tracker, Ads, Gaming, and Instant Messaging) can be done. Blocking a category or an application, user of ZenArmor can restrict certain applications as well as an entire category of applications. Preventing a programme by clicking on the green checkmarks on the left side of each application, users of ZenArmor can ban specific applications. Blocking an entire category, the user may also block an entire category by clicking the green tick mark next to the category name on the left.

5. RESULTS & DISCUSSION

The effectiveness of the ZenArmor in OPNsense is determined by its rules that have been set. This project evaluates the performance of ZenArmor to block and secure the network using three parameters Traffic Graph Throughput, Block local host, and Rules. Zen Console Cloud Threat Intelligence (CTI) is the process of gathering, examining, and disseminating knowledge about threats and vulnerabilities that target cloud environments in particular. It entails keeping an eye on and evaluating the security of cloud-based infrastructure, services, and systems in order to spot potential hazards and take preventative action to reduce them.

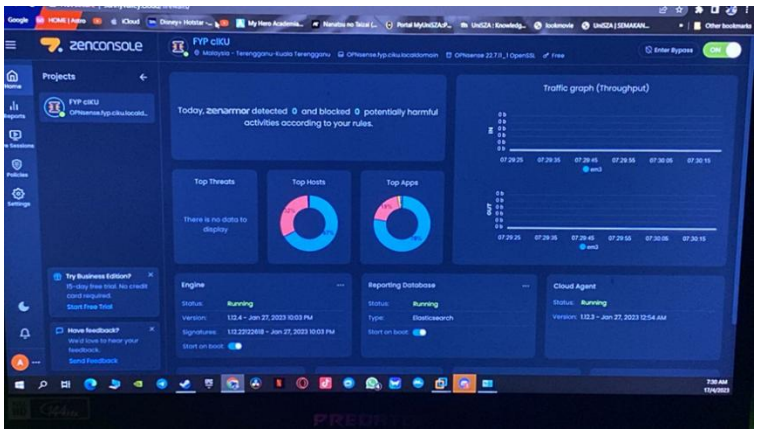

Figure 9 Live Review of Network Traffic using ZenConsole

Figure 9 cloud threat intelligence, organizations may strengthen their security posture by identifying and mitigating risks specific to cloud-based environments. The user can see a live view of all network traffic in the ZenConsole Dashboard.

Figure 10 Sample Throughput From ZenConsole

Figure 10 all network adapters for incoming and outgoing traffic is displayed in the upper portion of the screen. The graph will display real-time network movement. The physical infrastructure, network bandwidth, configuration options, and the particular plan or service being employed can all have an impact on ZenArmor's traffic throughput as shown in Figure 10. ZenArmor is made to process and manage network traffic effectively while guarding against DDoS assaults, flaws in web applications, and other security risks.

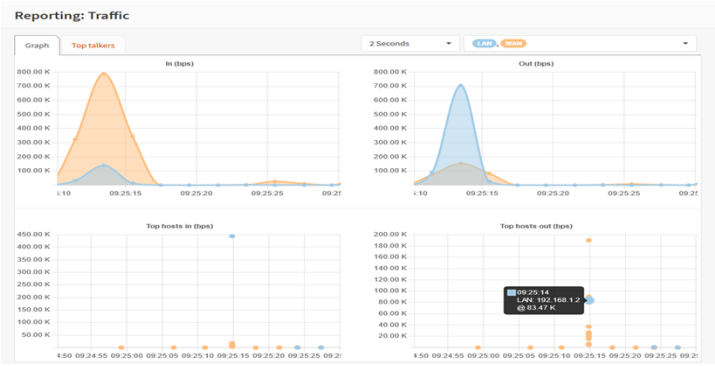

Figure 11 SampleTraffic Reporting From ZenConsole

Figure 11 exhibits the measured traffic volume and the most recent time traffic was seen from or to that address. With only one click, every network-connected device can be monitored. An overview of all network adapters for incoming and outgoing traffic is displayed in the upper portion of the screen. With the interface selection menu on the left, the user can choose the preferred polling resolution. In Figure 11, which shows the top consumers over the same time period, pointing to a dot reveals the measured bandwidth for the chosen host (the colour corresponds to the interface). It's important to remember that correct implementation, setup, and ongoing monitoring are necessary for ZenArmor or any other security solution to function effectively. To make sure they are appropriately secured against evolving cyber threats, organizations should examine their unique security needs, interact with specialists, and conduct frequent security assessments.

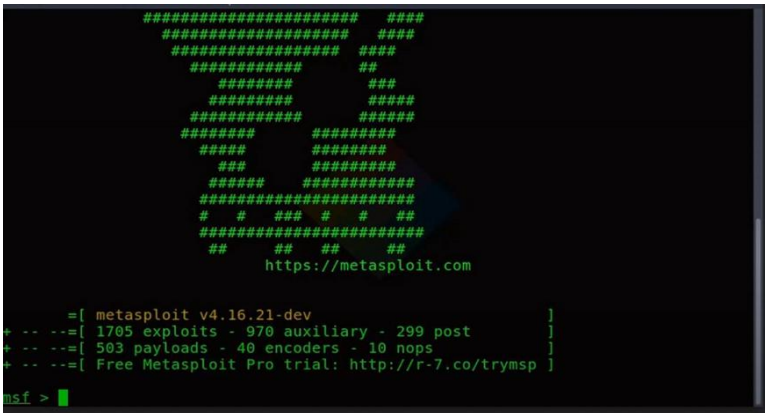

Figure 12 Sample Metasploit Attack Without OPNsense Turn On

Figure 12 shows an output of a penetration testing typically employed in addition to a web application firewall (WAF). If one works in cybersecurity, they won't only use Metasploit as a penetration testing tool. User should become familiar with a variety of utilities if user wants to become an expert in security. If OPNsense is activated, an attack cannot start. Because of suspicious activity that the firewall has detected.

6. CONCLUSION

In this paper, covered the project's testing and implementation. ZenArmor is a security solution developed by ZenLayer, a global software-defined network and cybersecurity provider. ZenArmor aims to protect networks, applications, and services from various cyber threats by leveraging advanced security measures. To evaluate ZenArmor's performance in safeguarding network traffic and guarding against various attacks, it underwent extensive testing. ZenArmor's capacity to identify and thwart unauthorized access, malicious activities, and data breaches was tested by replicating real-world events. In conclusion, ZenArmor showed outstanding performance, strong security features, and trustworthy threat detection capabilities. It worked well to defend network resources against a variety of threats while giving managers better control and visibility over network traffic. There are a number of improvements that may be made to future study that will increase the project's efficiency and effectiveness. First, SD-WAN that incorporates the cloud Given the rising popularity of cloud services and software-defined wide area networking (SD-WAN) solutions, efforts may be made to enhance OPNsense's interoperability and interaction with these platforms. This could simplify deployment, management, and security for hybrid and multi-cloud environments. Industrial Control Systems (ICS) with Internet of Things Support There may be efforts to build specific features and modules inside OPNsense to meet the particular security concerns given by the Internet of Things (IoT) and Industrial Control Systems (ICS) as they continue to grow. For IoT and ICS networks, this may incorporate features like network segmentation, device visibility, and policy enforcement.

References

[1] Shin, Y., 2019. Cross-VM cache timing attacks on virtualized network functions. IEICE TRANSACTIONS on Information and Systems, 102(9), pp.1874-1877.

[2] Kjorveziroski, V., 2021, May. Engaging Students with Personalized and Remotely Orchestrated Cybersecurity Training Exercises. In Proceedings of the 18th International Conference for Informatics and Information Technology (pp. 48-53).

[3] Koivunen, J. (2018) "Installing and Testing OpenSource Security Appliances", Metropolia Ammattikorkeakoulu, p. Available at: https://www.theseus.fi/handle/10024/157254

[4] Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. C. (2008). Influencing users towards better passwords: Persuasive cued click-points. *Proceedings of the 2008 Symposium on Usable Privacy and Security*, 1-12. DOI:10.1145/1531514.1531531

[5] Noorunnisa, Nahri & Siddiqui, Rahat. (2016). Review on Honey Encryption Technique. International Journal of Science and Research. 5. 1683-1686.

[6] Spitzner, L. (2002). Honeypots: Tracking Hackers. *Addison-Wesley Professional*, 480.

[7] Li, Z., Li, K., Zhou, W., & Chen, X. (2017). Enhancing Password Manager Security with Honeypots. Proceedings of the 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 1544-1549.
[8] Cai, Q., Zhang, W., & Gong, X. (2020). Analysis of Offline Brute Force Attacks on Password Managers. Journal of Information Security, 11(2), 69-81.