ISSN 2278-3091
Volume 9, No.1.3, 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse7291.32020.pdf
https://doi.org/10.30534/ijatcse/2020/7291.32020

Securing Network Using Raspberry Pi by Implementing VPN, Pi-Hole, and IPS (VPiSec)

Abidah Mat Taib[1], Mohammad Fikri Hanif Ishak[2], Nur Khairani Kamarudin[3], Mohamad Yusof Darus[4], Nor Azira Mohd Radzi[5]

[1]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Perlis, Malaysia, abidah@uitm.edu.my
[2]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Perlis, Malaysia, fikrihanif97@gmail.com
[3]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Perlis, Malaysia, nurkhairani @uitm.edu.my
[4]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Shah Alam, Malaysia, yusof_darus@uitm.edu.my
[5]Akademi Pengajian Bahasa Universiti Teknologi MARAPerlis, Malaysia, norazira202@uitm.edu.my

ABSTRACT

Every device on earth these days is associated with the Internet which brings humans an advancement of communication. Nonetheless, this technology discloses the user to the security threat. Barely users are sensitive that their data are being monitored by Internet Service Providers (ISPs) and other third-party companies. Furthermore, every webpage they visit, each information they fill in the search box are being monitored by a third-party company that wanted to know the user's interest and then will pop up advertisement which related to the user's interest. This turns into the issue when the third party has all the sensitive information and misuses it in unethical manners. Thus, it is the reason why a device that can protect the user is needed. A device with a capability to conceal the user's Internet Protocol (IP) and protect the user from any tracker and advertisement from the internet is proposed in this project. Hiding the user's IP address can be done by masking it with the OpenVPN server that is deployed in another country than making it safe for the user from being tracked by an attacker. Besides, blocking any Domain Name System (DNS) request for known tracking and advertising domain is achieved by using the Pi-Hole project that is being maintained by the online community. Along with that, the implementation of OSSEC IPS inside the Raspberry Pi has successfully prevented the brute force attack from inside the network to provide additional protection. The device with these integrated features is called VPiSec. Then, the network performance in terms of speed during the uploading and downloading before and after applying VPiSec is evaluated to see whether it is degraded. The findings show that there is no significant difference in terms of uploading and downloading speed without and with the application of WPiSec. Thus, users gained secure network activities while enjoying a smooth network performance.

Key words: Advertisement, attack, DNS, encryption, IPS, OpenVPN, Raspberry Pi.

1. INTRODUCTION

It is known that more than 53% of people are using internet activity actively. This value shows that more than half of people are connected to the internet, communicate with each other using the internet and making money with the internet which exposes them to the threat that can steal and exploit information from them [1][2]. One approach to defeating these vulnerabilities issues is by utilizing a Virtual Private Network (VPN). The word "network" refers to two or more devices that can communicate regardless of wired or wireless connection, as long as they can communicate and share data. The network has changed the way people live, as things that people used to do by hand formerly can now easily been done by computer and can be remotely controlled using the network.

Every device connected to a network; there are risks to security technology that must be addressed. These could include unauthorized access, Denial of Service (DoS) attacks and repurposing of a device by downloading malware, as with other devices attached to the network [4]. To avoid all of these attacks, few methods can be used by analysing types of attacks and implement the security tools. There are a few ways to protect the network environment either by the users itself, hardware and also applications used. Learning a few skills on using tools for securing networks can also help Internet users to ensure network security. Another way is by using hardware such as firewalls and IPS [5]. Besides implementing hardware, network security applications such as anti-virus, firewall and IPS software are also one of the ways users can use to secure network environments.

This paper presents an innovation of implementing a VPN router on a Raspberry Pi that is capable to encrypt the end-to-end connection between a user's device to servers so that the attacker cannot intercept the data [5][6]. Also, a

Pi-Hole is integrated into this project to block advertisements at the user's device. Pi-Hole works as a DNS sinkhole that blocks the queries contain advertisements from being forwarded to the internet, unlike ad-block which can only hide the advertisements and only work with supported browsers [4]. To add better security, OSSEC (open-source host-based intrusion detection system) IPS is also implemented in this project. Firewall functions as an intrusion prevention system (IPS), but IPS is focused on attack prevention on layers that most firewalls are not yet capable of deciphering [8]. The objective of this project is to develop a network tool that can secure the whole network environment from man-in-the-middle (MITM) attacks, adware, and any suspicious packets using Raspberry Pi technology. Then, experiments are carried out to evaluate the network tool system by testing its speed performance, several suspicious packets, and ads that can be blocked. This project is purposely designed for all internet users that want to keep their privacy and devices secured while travelling and want to avoid advertisements.

The rest of this paper is structured as follows: Section 2 talks about the literature review. Section 3 explains the methodology followed by testing and analysis in Section 4. Lastly, concluding remarks are presented in Section 5.

2. LITERATURE REVIEW

Some related works and terminologies are presented here to appreciate the importance of integrating several features in the proposed tool.

2.1 Virtual Private Network

Privacy is the most vital thing when it comes to network security. The purpose of a VPN is to provide security and privacy while communicating over the internet [5] [6] [9]. VPN is used to create a tunnel from the source device that is connected to the Internet using a VPN connection and encrypts all the data that is going through to avoid data leakage and being sniffed by unauthorized parties. A great option of VPN is to choose the open-source VPN as it can be customized according to the user's desire and supported by the community. OpenVPN is an open-source software application that implements VPN techniques between devices that are connected to the Internet. OpenVPN can transverse through firewalls and Network Address Translation (NAT). Moreover, OpenVPN is a cross-platform software that allows people to install and operate the software in various kinds of Operating System (OS). This is unlike any other VPN provider that always makes a VPN only for windows or Linux only. OpenVPN supports both Windows and Linux which makes it flexible and fully customizable. This project uses OpenVPN as it is widely used by the VPN community which provides many features and plugins to be configured with and helps a lot for doing this project.

2.2 Intrusion Prevention System

Network Intrusion Prevention Systems (IPS) has been developed to provide further protection as a response to the changing threat landscape. Beyond those offered by firewalls and Intrusion Detection Systems (IDS) which provide security but do not arrive at the point that IPS provides [7]. The IPS work is by going through the scanning of network traffic throughout the network, contrary to a system of intrusion detection that reacts solely, an intrusion prevention system is designed to prevent malicious events by preventing the attacks such as Denial of Service (DOS), Distributed Denial of Service (DDOS), exploits, worms and viruses [10].

2.3 Advertisement

Advertising is a means of communication with the users of a product or service whereas advertisements are messages paid for by those who send them and are intended to inform or influence people who receive them. These advertisements are very disturbing and annoying, some contain malware. Besides, they consume data and bandwidth which reduce the Internet.

A. Advertisement Blocker

Advertisement blocker or Adblock [6] is an extension or tool that can be used to block or restrict ads from popping up while browsing the Internet. Some Adblock has features that enable certain sites to be whitelisted and control its behaviour. Unfortunately, the tools are only compatible with the browser and anti-virus. This type of tool cannot block ads when the user is surfing the Internet using a smartphone or any other device. Therefore, the user is still exposed to threats and disturbed by the ads while using the Internet on other devices.

B. Pi-Hole

Mark Drobnak who is a college freshman of Rochester Institute of Technology has developed a way more powerful ad blocker named Pi-hole which they call "a black hole for advertisements" [11][12]. Most advertisement blockers need to be installed on different devices only, but the Pi-hole blocks ads across a whole network, including most applications. Pi-hole is intended to use on embedded devices with network capability such as Raspberry Pi.

There are different approach used by Adblock and Pi-hole to block ads. Adblock keep the web browser from viewing the ads from sites inside the browser. The ads are still being downloaded and still there but it is just being hidden by the Adblock. Pi-hole, on the other hand, does not even allow the Domain Name System (DNS) request for the ads to leave the

network, which means that the ads do not even get downloaded to the user's network

2.4 Raspberry Pi

As technology is radically evolving, the world now is experiencing smaller devices with a powerful performance at a cheaper price, namely Raspberry Pi. It is a well-known small-single board computer which commonly used by tinkers, programmers and computer students for general-purpose computer development [3] [13] and is suitable to be used in the Internet of Things (IoT) applications. The Raspberry Pi 3 Model B is the latest version of the Raspberry Pi computer and the most powerful among the other models of Raspberry Pi [17].

Securing network by using Raspberry Pi is being a popular topic that is discussed and developed by many researchers. One of the projects proposed using Raspberry Pi as a VPN server to a home network, to create a VPN connection between the home network and the public network. They use OpenVPN as their main VPN connection which then is set up inside Raspberry Pi [18].

According to Dirja and Rudi, they propose a project which provides an alternative solution for a security professional when using a public or free Wi-Fi. The project is using Raspberry Pi in conjunction with the freely distributed OpenVPN server and client software [16].

Another project uses Raspberry Pi as an advertisement black hole which prevents advertisement and popups from entering a user's network and prevents them from any unwanted malware attacks inside the online advertisement [17]. The project implements a DNS that rejects any request regarding advertisement, popups, irrelevant messages that wanted to go through the networks. The Pi-Hole is implemented inside the Raspberry Pi to work as the advertisement blocker. Another work, a NetGuard [5] has a similar purpose but it is featured with IDS that only alerts the detected attack but does not prevent it. However, this project implemented OSSEC IPS instead of the Suricata IDS which is capable of detecting the attack and preventing it.

3. METHODOLOGY

3.1 Design Phase

The design phase includes the use of a graphical scenario for the situation of the problem and the solution for the scenario. After that, an illustration diagram was used to illustrate the design of the system architecture. Figure 1 shows the graphical scenario of securing network connection using Raspberry Pi.

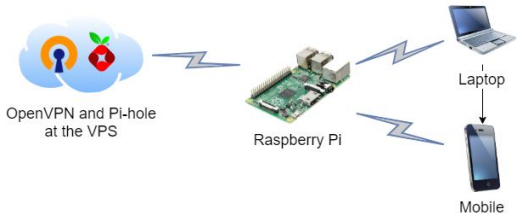

Figure 1: Graphical Scenario

This system required the Raspberry Pi to connect to the VPN that has been configured on the Virtual Private Server (VPS). Pi-hole was installed alongside the VPN. The user devices needed to be configured so that the default gateway for the devices can be sent to the Raspberry Pi. The system protected all data which travels through the VPN, as the Raspberry Pi blocked any suspicious packets using IPS. All the traffic that travelled into the user will be filtered to check for any known attacks or annoying online advertisements. The suspicious packets used IPS. All the traffic that travels into the user will be filtered to check for any known attacks or an annoying online advertisement. The user will feel safe and can safely surf the internet without having to worry about any data leakage or any type of attack.

An architecture system is a conceptual model that defines the structure, behaviour and explains more view of a system. It is a formal description and representation of a system, organize in a way that supports reasoning about the structures and behaviours of the system. A system architecture can comprise system components, the expand systems developed, the connection between the systems and other components that will work together to implement the overall system. Figure 2 shows the overall design of the proposed architecture for the VPiSec system.

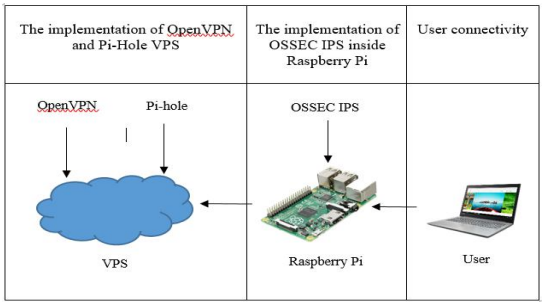

Figure 2: System Architecture

The Raspberry Pi 3 B was equipped with Raspbian as its Operating System. After the installation for the OS is finished, remote connection features were set up to ease user jobs to maintain the Raspberry Pi and to create the bridge connection between public Wi-Fi access and user's device.
The Raspberry Pi 3 B was installed with IPS and connected to the VPN that has been configured in the VPS. It was used to monitor all the traffics by logging and then block them. This project used OpenVPN as a VPN connection to secure and encrypt the data transferred by the user to ensure that the user

can safely browse the internet without worrying about the data being captured by the third party.

Next, the implementation of Pi-Hole inside the VPS alongside OpenVPN to block any DNS request regarding an online advertisement or tracking site is to ensure that users will not be disturbed by any annoying online advertisement and creating an ad-free environment.

Then, the Raspberry Pi 3 B will boot up using Raspbian which is a distribution of Linux for Raspberry Pi. The Raspberry Pi can be connected remotely using Putty after all the necessary configuration needed for remote connection has been set up. Virtual Network Computing (VNC) which is a graphical desktop sharing system could be used to control the desktop interface of the Raspberry Pi 3 B.

After that, OSSEC IPS [18] will be installed to the Raspberry Pi while setting it up to enable monitoring service and active response so that it will automatically block any suspicious packets.

3.2 Setting up OpenVPN and Pi-Hole inside Virtual Private Network

This project used the script made by FordSenpai on GitHub as the setup is much simpler compared to others. The script was modified to fit the project requirements. The OpenVPN was installed on Virtual Private Server (VPS).

Then, Pi-hole was installed on VPS as the ad-blocking mechanism. Installing Pi-hole involved few configurations to make sure that Pi-hole can work alongside the OpenVPN. Pi-hole was set up to be using the IP address of the tun0 interface in the OpenVPN network. This will enable the monitoring by the Pi-hole of incoming and outgoing traffic for the OpenVPN. VPS is also using the IP of the tun0 interface and selecting the same interface for the Pi-hole to work. Therefore, the desired IP address of the Pi-hole was configured as the IP address of tun0.

VPS was also using the IP of the tun0 interface and selecting the same interface for the Pi-hole to work. Therefore, the desired IP address of the Pi-hole was configured as the IP address of tun0.

Next, OpenVPN was configured to use custom DNS which is the Pi-hole DNS. OpenVPN server configuration file modified to push the Pi-hole IP as the DNS for the server configuration and comment out the other default DNS server to disable it.

3.3 Installation of OSSEC IPS OpenVPN client inside Raspberry Pi

Grafana script was used as they add more features like Loki and Prometheus to work alongside OSSEC. After installing OSSEC, Promtail was installed as the first component. After Promtail had been successfully installed, a configuration file was created and named as '*promtail.yml'* in the same directory.

Next, Loki was downloaded and installed to the Raspberry Pi. In the same directory of the installation, the configuration file was created and named as '*Loki-config.yaml'*.

Next, Prometheus was downloaded and installed. Then, the existing configuration file, 'prometheus.yml' was edited. After that, OpenVPN was installed on the Raspberry Pi for it to connect to the VPN server configured on VPS earlier. Last but not least, Grafana was downloaded and installed as the interface of the OSSEC. After all the components had been successfully installed, a start command for each of the components is entered to start all the components.

3.4 Implementation of OpenVPN, Pi-Hole, and OSSEC

The ovpn file that had been created while creating a new user is shared with the user's devices. User's devices were installed with OpenVPN client which is called OpenVPN Connect. The ovpn file then copied to the OpenVPN Connect. The user then connects the VPN using the ovpn file given and the login credential as configured and is directed to the OpenVPN server at the VPS.

Raspberry Pi was also connected to the VPN server so that all the packets that travel through it are encrypted and secured. An '*openvpn*' command entered to establish a connection between Raspberry Pi and OpenVPN. The terminal must be kept open to avoid the Raspberry Pi being disconnected from the VPN.

Next, the Raspberry Pi was needed to be set as the default gateway of the user's device. This ensures that any intrusion attempt on the device will be first monitored by the IPS inside the Raspberry Pi.

After the IP address of the Raspberry Pi has been set up as a device's default gateway, all the packets travelled from the device to the Internet will be tunnelled through the VPN and will be protected by the IPS. OSSEC can monitor and block any suspicious packets that were going through the network. Any communications made from the network is secured with an encrypted packet which allows user to browse the Internet without having to worry about data leakage or malware attack.

4. TESTING AND ANALYSIS

Three (3) main aspects are tested in this section. The first one is the anonymity of the user in the online world and the data sent from the user to the internet is readable in MiTM attack or not. The second test is testing the Pi-hole feature which is to block all the queries that matched the advertisement queries with the tracker queries that have been configured to the user's device while browsing the internet. The third test in analyzing the IPS that has been implemented inside the Raspberry Pi. Brute force attacks were conducted to the Raspberry Pi to see whether the OSSEC IPS is functional or not.

4.1 OpenVPN Anonymity and Leak Testing

In this section, two (2) types of testing are being executed to test the capability of the VPN in VPisec. Those are the IP address with a location leak test and DNS leak test to ensure that the users' location and DNS do not leak to the public.

A. IP Address and Location Leak Test

The first part of this testing is by using the tool with an existing internet connection without using OpenVPN. Figure 3 shows the result of the testing that indicates the user's IP address location is exposed. This exposure allows the attacker to trace the user's current location.

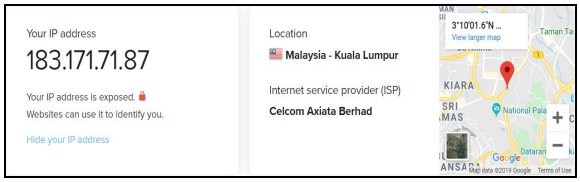

Figure 3: IP Address and Location Leak Test without VPN

The second part is using the tool after connecting to the implemented OpenVPN. The result as in Figure 4 shows that the ISP of the network has been replaced from Celcom to Digital Ocean which is the VPS used for the OpenVPN. Besides, the IP address has also been replaced with the IP address of the OpenVPN server which is also the IP address of the cloud server. In the tool display, it stated that the IP address is exposed, but it is the IP address given by Digital Ocean. The VPN hides the user and even the tool cannot detect if the user hides his/her IP with a VPN or not.

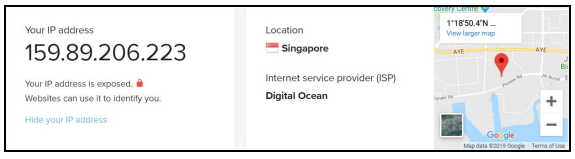

Figure 4: IP Address and Location Leak Test with VPN

B DNS Leak Test

In the beginning, the DNS leak test was tried on the network that is not connected to the VPN. Figure 5 shows the result of the DNS leak test which displays the DNS requests exposed. That means all the DNS requests made by the user while browsing the internet are possibly exposed to the ISP. ISP can track users' browsing and all the sensitive data sent and received. Besides, if there is a MITM attack to the ISP's DNS server, the attacker may also gain the users' sensitive data.

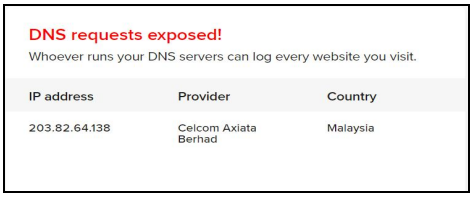

Figure 5: DNS Leak Test without VPN

Then, the test was conducted again after connecting the network to the VPN. The result in Figure 6 shows that the DNS provider has changed from the original ISP to Google and two DNS providers' addresses are leaked. The tool states that the DNS request is exposed because it does not know that the network has already being implemented and connected to the VPN to prevent DNS requests from being monitored and captured by ISP.

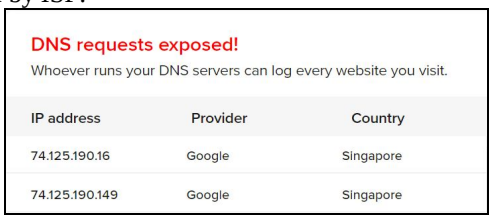

Figure 6: DNS Leak Test with VPN

4.2 Advertisement Blocking Testing with Pi-hole

The advertisement blocking test was conducted in two different states: - (i) on an application of a smartphone and (ii) using a web browser.

A. Pi-hole Testing with Application Installed on Smartphone

The testing was conducted on an application named SHAREit. SHAREit is an application that offers the user to share files and media with others. It is very popular because of its convenient and user-friendly. SHAREit is one of many applications that pops up an advertisement when the user opens it. It pops up immediately when the user opens the application, and when it is closed, another advertisement displayed on the homepage.

The application generates advertisement requests in the background and displayed them inside the application. This will not just distract the user, but will also consume more data and bandwidth for the application to request the advertisement and loads it to the user's smartphone. This operation also leads to a decreasing network performance because of its background process.

After the implementation of Pi-hole, the advertisement is no longer pops up when the user opens a SHAREit application. Besides, the homepage of the application also does not display annoying advertisements.

B. Pi-hole testing using Web Browser

The testing was conducted on the VocketFC.com that posts football news and content daily. The website was chosen because it displays so many annoying advertisements that distract the user while reading the content of the website. Fig. 7 shows an article posted on the website that contains several advertisements.

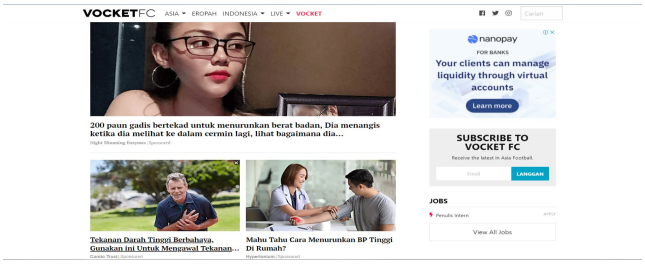

Figure 7: An Article on VocketFC.com that Contain Advertisements

As shown in Figure 7, the website displays so many advertisements that annoyed the user while reading the article. After Pi-hole is implemented, the result in Figure 8 shows that the same article on the website is no longer displays any advertisement.

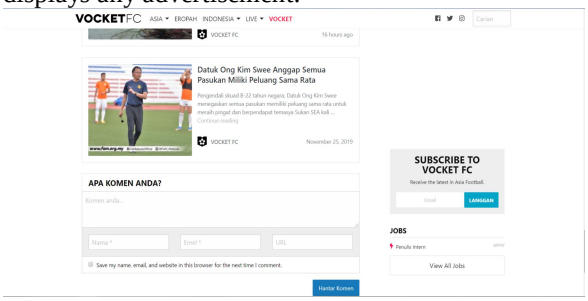

Figure 8: An Article on VocketFC.com after the Implementation of Pi-hole

Besides, the website loads faster than before the implementation of the Pi-hole. The proof of advertisement blockage can be seen on the output of Pi-hole GUI which is shown in Figure 9. That means Pi-hole has successfully blocked the query for advertisement from VocketFC.com. Thus, proved the capability of Pi-hole to block the advertisement on a website.

Figure 9: The output of Pi-hole GUI

4.3 OSSEC IPS Testing

This testing is conducted using a brute force attack to get the password of Raspberry Pi using Kali Linux. Without applying OSSEC IPS, the attack was successful and the attacker managed to guess the password and tried to control the victim remotely using ssh. On the other hand, with the OSSEC IPS on guard, the attack was unsuccessful. While OSSEC IPS is blocking any suspicious traffic, at the same time it actively logs all the activity that is happening inside the Raspberry Pi. Figure 10 shows the activity that has been logged by the OSSEC IPS.

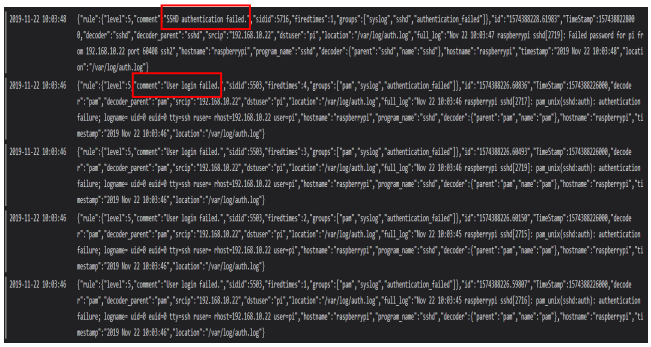

Figure 10: Logs of the Activity inside the Raspberry Pi

As in Fig 10, the OSSEC IPS logs that few failed attempts to log in to the Raspberry Pi. It shows that Kali Linux is using a brute force attack to guess the combination of passwords until it gets the right password. The login attempts are all logged and can be monitored by the user using OSSEC GUI. This will create awareness for the user that someone is trying to access the Raspberry Pi

5. RESULT AND ANALYSIS

Based on the testing and its result, it can be inferred that the outcome of this project helps the user to browse the Internet without any pop-up advertisement as it is blocked by implementing Pi-hole. Figure 11 shows the number of queries made by the websites and the number of advertisements that have been blocked in 1 day.

Figure 11: Number of Queries Blocked in 1 Day

Fig. 11 is the snippet from the Pi-hole GUI that shows the number of queries for the advertisement that have been captured and blocked by Pi-hole during Internet browsing by 5 users for 24 hours. During the browsing hour, a total of 1,437 queries have been made by 5 users and a total of 259 queries have been blocked. This shows that approximately 18% of the total queries contain advertisements and have been

successfully blocked by the Pi-hole in 1 day. Figure 12 shows the graph of blocked queries over the last 24 hours. The time graph shown is the result for the user browsing the Internet in 1 day. This shows that the Pi-hole capability is working perfectly fine to block advertisements in the network.

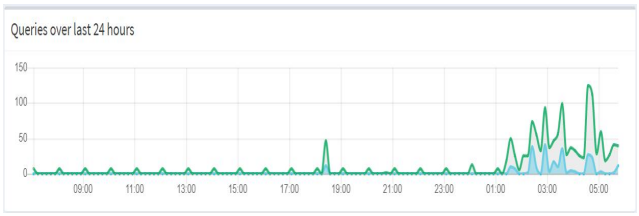

Figure 12: Queries Blocked over 24 Hours

Furthermore, OSEC IPS can block and at the same time log all the anomaly activities in the network. It also provides an alert rate. For instance, level 3 alerts refer to any successful or authorized events which include successful login attempts while level 7 alerts refer to bad word matching which includes "bad", "error", and others. Figure 13 shows the graph of level 7 alerts during the last 30 minutes of the network activity. It indicates that the brute force attack that was tested in the previous section is monitored and logged by the OSSEC IPS.

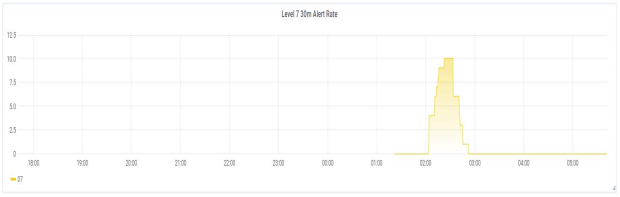

Figure 13: Level 7 Alert Rate due to Unsuccessful Login Attempt

Also, the network performance test was done to monitor the effect of using VPiSec which integrates VPN, Pi-hole, and IPS to the network. The test was done to check whether it will decrease network performance. This testing compares ping, download and upload speed before and after using all the features as they are the common measurements that the users care for to meet their satisfaction of using VPiSec. Table I shows the result of the testing.

Table 1: Result of the Testing To the Network Performance

Trial	Before using VPiSec			After using VPiSec		
	Ping (ms)	*Download (Mbps)*	*Upload (Mbps)*	*Ping (ms)*	*Download (Mbps)*	*Upload (Mbps)*
1	25	19.75	28.69	37	17.07	12.35
2	29	27.35	18.47	38	14.84	23.29
3	25	30.98	17.56	38	14.22	23.13
4	27	15.08	24.23	38	17.92	27.88
5	26	20.37	29.27	37	14.92	32.35

The result of the network performance after using the project slightly decreased in terms of download speed before using the project. However, the upload speed showed a slight increase after using the project compared before using it in the last 4 trials. These showed that the project might affect a little bit of the users' experience in downloading content from the Internet but gives a better upload speed to the users. Meanwhile, the ping results showed that VPiSec increases the time in requesting and responding messages.

Nevertheless, a paired T-test has been conducted to check whether there is a significant difference before and after implementing the VPiSec. This is shown by using $\alpha = 0.05$, H_0 : after = before. The result showed in Table 2 the calculated p-value was greater than α, which concluded that the speed has no significant difference in downloading and uploading activities before and after implementing the VPiSec. However, for ping activity, it produces a significant difference since the p-value is smaller than α. It confirms that VPiSec gave a slight impact on ping. This might affect users' experience, especially in gaming. However, a ping rate from 20 to 100 ms will still get to enjoy the gameplay, but might not give maximum performance for games where timing is everything [19].

Table 2: P-Value for Paired T-Test

P-value		
Download	Upload	Ping
0.1187	0.9718	0.0001

6. CONCLUSION

The configuration for VPiSec is simple as it is designed to ensure that even novice users can use and implement it to secure their network. The user connects with the VPiSec which acts as an intermediary for the user and the Internet. The experiments were done on the VPiSec to test the functionality of the OpenVPN, Pi-hole and OSSEC IPS. The test done on OpenVPN showed that user IP and location were hidden which means that it is successfully working. Besides, the test done on Pi-hole showed that advertisements had successfully blocked applications and also on websites. If there is a new site tracker query that is being created by advertisement services, then the user needs to update the blocklist to make sure that Pi-hole can keep blocking advertisements. Next, the OSSEC IPS implemented inside the VPiSec was showing logs on anomaly activities inside the VPiSec. It successfully blocked intrusion attempts and only protect the user within the same network as the VPiSec. It will not monitor or block any activities that are beyond the network. The network environment will only be secured if the user uses the VPiSec as its default gateway. In conclusion,

VPiSec helps internet users to secure their network activities. This project suggests improving a command that can make Pi-hole updates its database automatically. Also, modifies the router configuration for the IP table to route all the traffic that goes into the router that also goes to the VPiSec.

REFERENCES

1. M. A. Elsadig, A. Altigani, M. A. Ali Baraka. **Security Issues and Challenges on Wireless Sensor Networks.** *International Journal of Advanced Trends in Computer* Science and Engineering, 8(4), July- August 2019, 1551 – 1559
2. D. Rani, N. S. Gill. **Lightweight Security Protocols for the Internet of Things: A Review**. *International Journal of Advanced Trends in Computer Science and Engineering*, 8(3), May - June 2019, 707 – 719.
3. V. Osamor, O. Emebo, B. Fori, M. Adewale. **Engineering and Deploying a Cheap Recognition Security System on a Raspberry Pi Platform for a rural Settlement**. *International Journal of Advanced Trends in Computer Science and Engineering*, 8(6), November - December 2019, 2904- 2909.
4. P. Garms and S. MurphySep, **Consider Data Security**, *Security Today*, 01-Sep-2018. [Online]. Available: https://securitytoday.com/articles/2018/09/01/consider-data-security.aspx?admgarea=ht.networkcentric. [Accessed: 14-Apr-2019].
5. F.M. Rustono, D.G.S Achmad, D. Agus, S. Wa Ode, P.M. Alfred. **Information Security Risk and Management in Organizational Network**. International *Journal of Engineering and Advanced Technology (IJEAT).* Volume-8 Issue-6S2, August 2019.
6. A. Mat Taib, M. Tholhah Zabri, N. A. Mohd Razi, E. Abdul Kadir. "**NetGuard; Securing Network Environment using Integrated OpenVPN,-Pi-Hole, and IDS on Raspberry Pi**. International Conference on the future of ASEAN. 2019.
7. S. Taylor, **VPN Ad Blockers - The Best and the Worst**," Restore Privacy, 20-Sep-2019. [Online]. Available: https://restoreprivacy.com/vpn-ad-blocker-comparison/. [Accessed: 27-Mar-2019].
8. A. A. Amjad and N. H. O. Hebah, Intrusion Prevention System, vol. 3, no. 1, pp. 432–434, Jan. 2011.
9. H. Tasmi, D. Setiawan, D. Stiawan, S. Husnawati, Analar Valiata. **Determining Attributes of Encrypted Data Traffic Using Feature Selection Method**. *International Journal of Engineering and Advanced Technology (IJEAT).* Volume-9, Issue-1, October 2019.
10. S. Wilkins, ***Basic Intrusion Prevention System (IPS) Concepts and Configuration***, *Cisco Press, 29-Jun-2011. [Online]*. Available: http://www.ciscopress.com/articles/article.asp?p=1722559. [Accessed: 15-Apr-2019].
11. A. Jeffries, **Inside the Brotherhood of the Ad Blockers**, Bloomberg.com, 10-May-2018. [Online]. Available: https://www.bloomberg.com/news/features/2018-05-10/inside-the-brotherhood-of-pi-hole-ad-blockers. [Accessed: 21-Apr-2019].
12. J. C. Dunn. **Using a Raspberry Pi for Network Protection and Data Collection**. Master Of Science In Applied Engineering And Technology Management. Eastern Kentucky University. 2018. Accessed on: 6 Jan 2020. Available: http://www.eku-aet.org/net/Capstone/2019/JoshuaDunn_EKU_NET_Graduate2019_report.pdf.
13. N., Heath. **What is the Raspberry Pi 3? Everything You Need To Know About The Tiny, Low-cost Computer | ZDNet.** ZDNet. (2017, November 30). Retrieved November 28, 2019, from https://www.zdnet.com/article/what-is-the-raspberry-pi-3-everything-you-need-to-know-about-the-tiny-low-cost-computer
14. W. Gary (2014). **Raspberry Pi Hardware Reference. Technology in Action**. Retrieved from https://www.raspberrypi.org/.
15. E. Jodoin, **SOHO RemoteAccess VPN. Easy as Pies, Raspberry Pi**, *SANS Institute Reading Room*, 41. 6 Jan 2020. Available: https://www.sans.org/reading-room/whitepapers/networkdevs/soho-remote-access-vpn-easy-pie-raspberry-pi-34427
16. Dirja Nur Ilham, Rudi Arif Candra. **Analisis Celah Keamanan Jaringan Komputer Dengan Menggunakan Raspberry Pi 2.** *METHOMIKA: Jurnal Management Informatika & Komputerisasi Akuntansi*. Vol. 2 No. 2 (Oktober 2018). ISSN: 2598 – 8565. Available: http://www.methomika.net/index.php/jmika/article/view/50/47.
17. Shyam Nandan Kumar, Amit Vajpayee. **A Survey on Secure Cloud: Security and Privacy in Cloud Computing**. *American Journal of Systems and Software*, 2016, Vol. 4, No. 1, 14-26 Available online at http://pubs.sciepub.com/ajss/4/1/2 © Science and Education Publishing.
18. D. Teixeira, L. Assunção, T. Pereira, S. Malta, P.Pinto **OSSEC IDS Extension to Improve Log Analysis and Override False Positive or Negative Detections**, *Journal of Sensor and Actuator Networks*, 2019, 8,46.
19. S. C. Madanapalli, H. H. Gharakheili, V. Sivaraman. **Assisting Delay and Bandwidth Sensitive Applications in a Self-Driving Network**. NetAI '19, August 23, 2019, Beijing, China © 2019 Association for Computing Machinery. ACM ISBN 978-1-4503-6872-8/19/08. https://doi.org/10.1145/3341216.3342215.