Stealthy Personal VPN Connection

Nithin Steward Raj N. D
Cloud Technology and Information Security
Rathinam College Of Arts and Science
Coimbatore,Tamilnadu, India

Uvan Sankar N
Cloud Technology and Information Security
Rathinam College Of Arts and Science
Coimbatore,Tamilnadu, India

Gayathri M
Cloud Technology and Information Security
Rathinam College Of Arts and Science
Coimbatore,Tamilnadu, India

***Abstract*—the Internet provides enormous facilities like online banking, online shopping, communications, businesses, and organisations. This leads to the requirement of securing a communication network. Nowadays, most software collects user data to make them consistent users by suggestions, ads, and push notifications based on the user data. There is a major threat of data breaches in such cases. Thus, masking such information over internet searches and using any other applications is needed. The project aims to design a Personal Virtual Private Network for Internal Home Networks using Raspberry Pi as a VPN server with the LAN gateway or the router. This system can mask the source of data that is being generated on the internal network. This system tries to solve the problem of sharing user data over the internet and helps to prevent the most common security threat of data breaches. This project also aims to block the ads, thus preventing phishing attacks. To filter the incoming traffic from any anomalies, Intrusion Detection System and an Intrusion Prevention System have been included.**

Keywords—VPN server, Raspberry Pi, IoT, IPS, HoneyPot

I. Introduction (*Heading 1*)

Virtual Private Networks (VPNs) have become a vital tool for securing and protecting the privacy of data transmitted over the internet. However, VPNs alone are not sufficient to secure networks, as they are susceptible to intrusion and hacking attempts. To tackle this issue, many organizations are now combining VPNs with Intrusion Prevention Systems (IPS) to increase the overall security of their networks.

This paper presents an integration of Pi VPN, a popular open-source VPN solution, with an IPS to create an Integrated Pi VPN system. The study aims to investigate the benefits and drawbacks of implementing an IPS within a VPN system and to evaluate the effectiveness of the Integrated Pi VPN system in protecting networks against hacking attempts and intrusions.

The paper covers the design and implementation of the Integrated Pi VPN system and its performance evaluation through a series of tests and simulations. The results of these tests and simulations will be analysed and discussed in detail, and recommendations will be made for future improvements and optimizations.

This research paper contributes to the field of network security by providing insights into the implementation and performance of Integrated Pi VPN systems, and by offering a practical solution for organizations looking to secure their networks with a VPN and IPS combination.

II. Literature Survey

A. *Virtual Private Network*

When it comes to network security, privacy is everything. A VPN's objective is to give security and anonymity when communicating over the internet. VPN is used to build a tunnel from a source device that is linked to the Internet through a VPN connection and encrypts all data passing through to prevent data leakage and sniffing by unauthorised parties. Open-source VPN is an excellent alternative since it can be adjusted to the user's preferences and is maintained by the community. Open VPN is an open-source software tool that enables VPN protocols between Internet-connected devices. Open VPN can pass through firewalls and Network Address Translation (NAT). Furthermore, Open VPN is a cross-platform program that can be installed and used in a variety of operating systems (OS). This is in contrast to any other VPN service, which always creates a VPN that is only available for Windows or Linux. Open VPN supports both Windows and Linux, making it versatile and completely adaptable. This project employs Open VPN since it is extensively used by the VPN community and gives many features and plugins to set up, which greatly aids in the completion of this project.

B. *Intrusion Prevention System*

In response to the increasing threat landscape, Network Intrusion Prevention Systems (IPS) have been created to give additional security. Beyond the capabilities of firewalls and Intrusion Detection Systems (IDS), which provide protection but do not reach the level of IPS. In contrast to an Intrusion Detection System (IDS) that just reacts, an intrusion prevention system is meant to prevent hostile events such as Denial of Service (DOS), Distributed Denial of Service (DDOS), exploits, worms, and viruses by analysing network traffic throughout the network.

C. *Advertisement Blocker*

Advertisement is a method of communicating with users of a product or service, whereas advertising is communications paid for by those who send them and intended to inform or persuade those who receive them. These adverts are incredibly upsetting and unpleasant, and some of them include viruses. Furthermore, they use data and bandwidth, which slows down the Internet.

Advertisement blocker, often known as Ad block, is a browser plugin or program that may be used to prevent advertisements from appearing when browsing the Internet. Some Ad Block products have capabilities that allow specific websites to be whitelisted and manage their behaviour. Unfortunately, the tools only work with the browser and anti-virus software. This sort of solution cannot prevent advertisements when the user is browsing the Internet on a smartphone or other device. As a result, while surfing the Internet on other devices, the user is still exposed to risks and bothered by advertisements.

D. *Pi-hole*

Mark Drobnak, who is a college freshman at Rochester Institute of Technology has invented a far more effective ad blocker termed Pi-hole which they call "a black hole for adverts". Most advertisement blockers need installation on individual devices, whereas the Pi-hole prevents adverts over an entire network, including most apps. i-hole is intended for usage on network-capable embedded devices such as the

Raspberry Pi. Ad block and Pi-hole use distinct approaches to ad blocking. Ad block prevents the web browser from displaying adverts from websites within the browser. The advertisements are still being downloaded and displayed, but they are being obscured by Ad Block. The adverts do not even be downloaded to the user's network because Pi-hole, on the other side, prevents the Domain Name System (DNS) request for the ads to exit the network.

E. Raspberry Pi

As technology advances, the world is seeing smaller gadgets with tremendous capabilities at a lower cost, such as the Raspberry Pi. It is a well-known compact, single-board computer that is frequently used by hackers, programmers, and computer students for general-purpose computer development and is appropriate for usage in Internet of Things (IoT) applications. The Raspberry Pi 3 Model B is the most recent version of the Raspberry Pi computer and the most powerful of the Raspberry Pi series.

Securing networks with Raspberry Pi is a hot issue that many academics are discussing and developing. One proposal suggested utilising a Raspberry Pi as a VPN server for a home network to establish a VPN link between the private network at home and the public network. They utilise Open VPN as their primary VPN connection, which is then configured on the Raspberry Pi. Dirja and Rudi suggest a concept that offers an alternate approach for a security professional when accessing public or free Wi-Fi. The Raspberry Pi is being used in combination with the publicly available Open VPN server and client software.

Another project employs the Raspberry Pi as an advertisement black hole, preventing advertisements and popups from accessing a user's network and protecting them from unwanted virus assaults within the online advertisement. The project develops a DNS that refuses any request for an advertisement, popups, or unnecessary data to pass through the networks. The Pi-Hole is an advertising blocker that is built into the Raspberry Pi. Another effort, a Net Guard, serves a similar function, but it includes IDS, which only warns of the identified assault and does not prevent it. However, instead of the Suricata IDS, which is capable of detecting and stopping the attack, this project used OSSEC IPS.

III. Methodology

A. VPN Script

A custom VPN Script was implemented that is specifically designed to meet the unique requirement of hiding the client information even from the VPN service provider. It gives us full control over the script's functionality and behaviour and avoids detection or Spoofing by the ISP. The script may increase the latency by 30%, it can be solved if the Internet connection is faster than 30 Mbps per order. The connection between the client/user is secured and it cannot be attacked or spoofed or spied on. The connection uses Advanced Encryption Standard (AES) for encrypting. AES 256 is a virtually impenetrable symmetric encryption algorithm that uses a 256-bit key to convert your plain text or data into a cipher. This encryption standard is also used by the Military in some countries for securing their communication.

B. Port Forwarding

It is a technique used to allow remote access to a computer or device on a private network. In a Raspberry Pi, port forwarding can be set up to allow external devices to access services running on the Raspberry Pi, such as a web server or SSH service. By configuring Port Forwarding we can forward all the traffic through the Raspbian Pi. With port forwarding, we can monitor all the traffic that takes place in the network. By monitoring network traffic for specific ports to ensure that the expected traffic is flowing through them. This can help detect potential security threats, such as unauthorized access attempts, and ensure that network performance is not being impacted by unexpected traffic.

C. Intrusion Detection System

Network traffic is monitored by an intrusion detection system (IDS), which warns users when it detects any unusual activity. Software is included in the Raspberry Pi, which is used to look for malicious activity or policy violations on a system or network. Using a Security Information and Event Management (SIEM) system, any illegal activity or violation is frequently logged centrally and reported to an administrator. This system combines the outputs from several sources and uses alarm filtering techniques to separate valid alarms from false alarms.

D. Intrusion Prevention System

IPS is also known as an Intrusion Prevention System. It is a network security application that monitors network or computer activity for malicious activity. The main functions of intrusion detection and prevention systems in Raspberry Pi are to detect malicious activity, collect information about this activity, and attempt to prevent or stop it. Intrusion detection and prevention systems are deployed in our VPN-enabled network with high traffic and networks that need higher security.

E. System Design

The VPN script executes and makes the connection using AES 256 encryption and creates an SSL tunnel peer connection. It makes the connection a bit slower as the encryption and other process needs to take place, this process affects the latency by 30% user may experience a bit of lag or stutter during the initial connection. The traffic flows through the Raspbian and then to the router and gets to ISP in a single port which is encrypted and secure. Then the traffic reaches the Internet. All the end devices that are connected to the Pi will be protected and the traffic will be monitored and logged. The IDS can generate an alert that set a beep audio alerting the admin at the time of an intrusion.

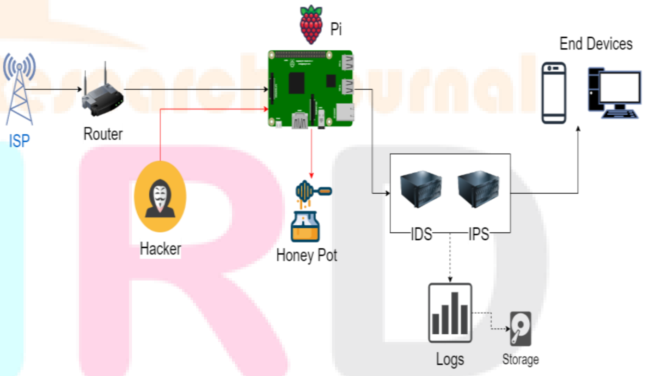


Figure 1: Overview of the proposed system

IV. Experimental Setup

A. Raspbian Setup

User OS and version are detected while running the script. The user is asked to choose the DNS server gateway is chosen. All IP-related information is being set and the client configuration file is being configured. Installing a module for generating QR code with the created configuration file. A firewall is being configured, if the firewall is installed. Otherwise, install a firewall and then configure, it if not installed.

B. Bash Scripting For Configuring VPN

Start and run the bash script file (file.sh), the reason why we are using bash is the environment that we are using is a

Linux system. So bash communicates directly to the kernel, making the operation so much faster and more efficient. and user OS and version are detected while running the script. The user is asked to choose the DNS server gateway is chosen. All IP-related information is being set and the client configuration file is being configured. Installing a module for generating QR code with the created configuration file. A firewall is configured if the firewall is installed or else install a firewall. This is the basic overview of the script running. It's better than the normal VPN that our script tells the OS or the Browser that the user is using and it has additional security features combined with it.

C. *Honeypot*

A honeypot is a security mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities so you can study them to improve your security policies. Our Honey Pot is a Low interaction honeypot that gives very little insight and control to the hacker about the network. It simulates only the services that are frequently requested by the attackers. The main operating system is not involved in the low interaction systems and therefore it is less risky. They require very fewer resources and are easy to deploy. The only disadvantage of these honeypots lies in the fact that experienced hackers can easily identify these honeypots and can avoid them. Our Honey Pot mimics a vulnerable system to distract and detect attackers. And it logs the user activity and the IP can be blocked to prevent further attacks.

D. *Intrusion Prevention & Detection System*

The Raspberry Pi can detect and alert to malicious activity or potential security threats. It acts as an additional layer of security for the home network, helping to detect and respond to security threats that other security measures may miss.

E. *Enable VPN Server*

You can download the VPN script and required files from any of the links

https://github.com/NithinStewardRaj/Final_year_project-

https://github.com/MGayathri360/UG_Academic_Project

https://github.com/Uvansankar2003/FinalYear-project

Hosting the file in GitHub makes it easy to download and configure and give execute permission to the script file and execute the file.

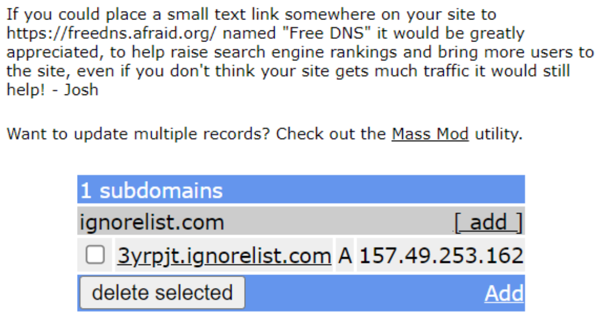
F. *Remote Access Of Raspberry Pi*

We can get remote access to our Raspberry Pi using SSH. For more Security, we can disable root login and allow login using SSH key-based authentication only. Result And Conclusion

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll-down window on the left of the MS Word Formatting toolbar.

V. Result And Discussion

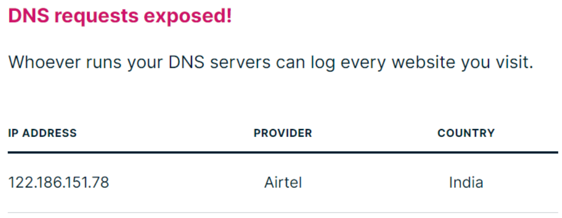
A Bash Script is used to connect with the VPN service. Here we created a custom Bash script and With the VPN Script running we are connected to the VPN service and all the outbound traffic is encrypted and secured. All the Network activity is logged. We can see the Location and IP leaked in Figure (Fig 6.1) and figure (Fig 6.2) shows the IP and location changed. DNS leak test is done without VPN and with VPN. From IDS and IPS, we can detect and block most of the attacks. An attacker tries to do a Nmap scan and we can see open ports. If the attacker tries to access any of the ports an alert is created and logged.


If you could place a small text link somewhere on your site to https://freedns.afraid.org/ named "Free DNS" it would be greatly appreciated, to help raise search engine rankings and bring more users to the site, even if you don't think your site gets much traffic it would still help! - Josh

Want to update multiple records? Check out the Mass Mod utility.

1 subdomains	
ignorelist.com	[add]
□ 3yrpjt.ignorelist.com A 157.49.253.162	
delete selected	Add

Figure 2.1: DNS


DNS requests exposed!

Whoever runs your DNS servers can log every website you visit.

IP ADDRESS	PROVIDER	COUNTRY
122.186.151.78	Airtel	India

Figure 2.2: DNS leak

VI. Conclusion

The research paper explores the potential for integrating Pi VPN with an Intrusion Prevention System (IPS) to increase the overall security of the VPN. The study covers the design and implementation of the Integrated Pi VPN system and its performance evaluation.

By providing an in-depth study of Pi VPN and its integration with an IPS, this research paper contributes to the field of network security by offering a practical solution for organizations looking to secure their networks and protect sensitive information.

A. *Limitations*

In case of low internet bandwidth, there is a chance of latency. Peer connection may not be established. Thus, the detection of any anomalies in the system may be delayed which leads to the risk of cyber-attacks.

B. *Future Work*

For making it more user-friendly by integrating this system with an Interface. That means this can also be implemented as accessing via Graphical User Interface (GUI).

Based on the results of the performance evaluation, the paper provides recommendations for future improvements and optimization of Pi VPN, including the integration of additional security tools and the implementation of advanced encryption algorithms.

Acknowledgement

This paper and the research behind it would not have been possible without the exceptional support of our supervisor, Mr

Vignesh S M. Tech., M.B.A., and our project coordinator, Dr P.K.A. Chitra M.E., PhD. Their enthusiasm, knowledge, and exacting attention to detail have been an inspiration and kept our work on track till the final draft of this paper.

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] 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]

[3] 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.

[4] 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].

[5] 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/sohoremote-access-vpn-easy-pie-raspberry-pi-34427Y.