Eximia Journal

(ISSN 2784-0735)

Vol. 12

2023

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Safeguarding Transactional Data: A Comprehensive Investigation of VPN Integration in Point-of-Sale Systems for Enhanced Security and Connectivity

Loreto B. Damasco Jr., Noel Raymund F. Lacson, Roger T. Intong

University of St. La Salle

l.damasco@usls.edu.ph, nr_lacson@usls.edu.ph, r.intong@usls.edu.ph

Abstract. The integration of Virtual Private Network (VPN) technology into Point-of-Sale (POS) systems has emerged as a solution for securing transactional data in businesses. This study investigates the implementation of a VPN server to address security and connectivity challenges faced by the University of St. La Salle (USLS) Bookstore. The research delves into VPN policy frameworks, assessing the scope and binding, authentication methods, and VPN credentials and security protocols. The system design employs a combination of conceptual models and activity diagrams to illustrate the process of user authentication and data encryption. Furthermore, the study evaluates the system's performance in terms of scalability, efficiency, and effectiveness in ensuring authentication and security. The deployment of the VPN infrastructure involves the installation of requisite software and hardware components, along with rigorous testing procedures to assess system performance and reliability. The findings highlight the significance of VPN in safeguarding sensitive transaction data and enhancing the efficiency of POS operations. The study's outcomes offer valuable insights into the effective implementation and management of VPN technology for securing business operations.

Keywords. Virtual Private Network, Point-of-Sale System, Encryption, Authentication, Network Security

1. Introduction

In the current digital landscape, ensuring the security and privacy of online activities has become a paramount concern. Virtual Private Network (VPN) technology has emerged as a critical solution to safeguarding sensitive data and enhancing network security. By rerouting connections through secure servers and encrypting user data, VPNs provide a shield against potential threats, allowing users to access the web safely and securely (Mardisalu 2019). According to the study conducted by (Iqbal & Riadi, 2019), Virtual Private Networks (VPNs) play a crucial role in ensuring secure communication and protecting valuable information from potential hacker attacks. By employing encryption techniques and tunneling technology, VPNs facilitate the transmission of encrypted data across various networks (Faircloth 2017), providing a robust shield against cyber threats (Borky JM 2018). The encryption process, often employing algorithms such as the Advanced Encryption Standard (AES) with a minimum of 128 bits, ensures the protection of sensitive information (Mardisalu, 2019).

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Moreover, the integration of VPNs within Point-of-Sale (POS) systems has proven to be instrumental in securing transactions and data. By installing VPN client software at each branch, the VPN server and POS server work in tandem, allowing authorized access to the POS application only after authentication by the VPN server. This setup not only hides user transactions and encrypts data but also facilitates centralized data collation, eliminating the need for manual copying of files from various branches (Entrepreneur Asia Pacific, 2019).

The implementation of VPNs within the context of a bookstore's operations, as highlighted in this study, underscores the critical need for secure network connections, especially in handling sales transactions and managing inventory. The traditional process of entering stock data into a cash register and generating daily reports poses several limitations, including manual data entry and the need for physical visits in the case of system breakdowns. By introducing VPN technology, these challenges can be effectively addressed, ensuring secure and efficient data management across multiple branches.

Furthermore, the increasing prevalence of VPNs within educational institutions emphasizes the growing importance of network security in the academic setting (Xiong 2019). With VPNs serving as a protective barrier against unauthorized access and data breaches (Borky and Bradley 2018), educational institutions can create a closed network space, allowing students secure access to campus resources while off-site. The use of data encryption technology, network data tunneling, and user authentication technology within the context of VPNs enhances overall information security and strengthens the management of computers and network resources within campus environments (Karaymeh et al 2019).

As the internet continues to evolve, the importance of VPNs in ensuring safe connections and protecting sensitive data remains a pivotal consideration across various sectors (Prasad et al 2016). This paper seeks to delve into the multifaceted applications of VPNs and their significance in creating secure network connections in the modern digital age. By examining the various protocols and encryption techniques used by VPNs, we aim to shed light on their robust capabilities and their potential for enhancing communication security and privacy.

2. Materials and Methods

In preparation for gathering results, the researchers employed one VPN server and three clients. The VPN server utilized the Centos 7 operating system (OS), VPN services, and applications, responsible for client authentication through VPN. Among the clients, one functioned as the POS server while the others served as POS clients. With authorization from the bookstore, the researchers utilized their existing POS system data for testing. The testing of servers and clients was conducted utilizing the university's network infrastructure, as permitted by the ITS director.

The researchers generated 11 user accounts for the three VPN clients, requiring the specification of their usernames. Three of the clients underwent testing in the ITS office, while the remaining clients were tested in the computer research laboratory. Additionally, the researchers implemented the Fail2Ban application to safeguard the server from potential DDoS attacks. This application was initiated as a service, and the generated logs were recorded. The server certificate, user certificates, and user keys were replicated and distributed to the client. These files were employed to configure the OpenVPN application to establish a connection with the server. On the client side, the researchers initiated the OpenVPN application to connect to the server.

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Following successful user authentication, the researchers scrutinized the server logs to identify the Internet Protocol (IP) address provided by the server. The researchers then logged into the POS system and executed various POS transactions. All activities, ranging from authentication to the POS transactions, were meticulously logged by the VPN server. By utilizing Wireshark, the researchers viewed and documented VPN logs as screenshots. The researchers also attempted to connect the VPN client to the VPN server using invalid credentials. All logs were subsequently analyzed and interpreted by the researchers to ascertain their alignment with the study's objectives.

The three (3) respondents of the study comprised the personnel of the USLS responsible for maintaining and monitoring the network infrastructure. The researchers conducted an extensive technical examination, formulating a survey questionnaire for use by other technical experts to validate the testing results. The Likert 5-point scale was employed to interpret the respondents' feedback concerning the system's quality evaluation.

The content validation was conducted to assess the extent to which the test items reflected the anticipated subject matter content. In pursuit of this objective, three (3) experts in the relevant field adjusted the instrument by making alterations to a few items and proposed the necessity of translating the instrument into the local dialect. The Good and Scates validation form was employed to evaluate the content validity of the instrument, resulting in a validity rating of 4.6, which was interpreted as valid.

Reliability testing was not included in this study since the survey questionnaire was solely utilized to validate the results of the testing process. Upon the retrieval of survey instruments from the participants, the data were tabulated, tallied, analyzed, and interpreted, ultimately presented in a tabular format. The interpretation of the collected data employed the use of the weighted mean, given that the stipulated issues were entirely descriptive in nature.

Ethical Consideration

The system was specifically designed to enhance the security of the POS system. In this context, the researchers scheduled an appointment with the director of the USLS bookstore and the POS Admin for an interview, aiming to gain familiarity with the functioning of the POS. Subsequently, the researchers submitted a letter of intent to the Information and Technology Services (ITS) director for approval. Following this, the researchers and the ITS office mutually agreed upon the terms and conditions for the implementation of the system.

System Design

The conceptual design of the VPN implementation encompassed the integration of various illustrative tools, including the use case diagram, activity diagram, system architecture, software specifications, hardware specifications, system implementation, system testing, and deployment. The Use case diagram was instrumental in representing the system, composed of the business actors and use cases. The business actor assumed the role of a person or any system within the business model that interacted with the system. The use case diagram, depicted in Figure 1, included three primary actors: the user, administrator, and the VPN server. For the user, the use cases comprised VPN login and logout, POS login and logout, and POS transactions. Meanwhile, under the VPN server, the use cases involved VPN user authentication and logging of VPN user activities.

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

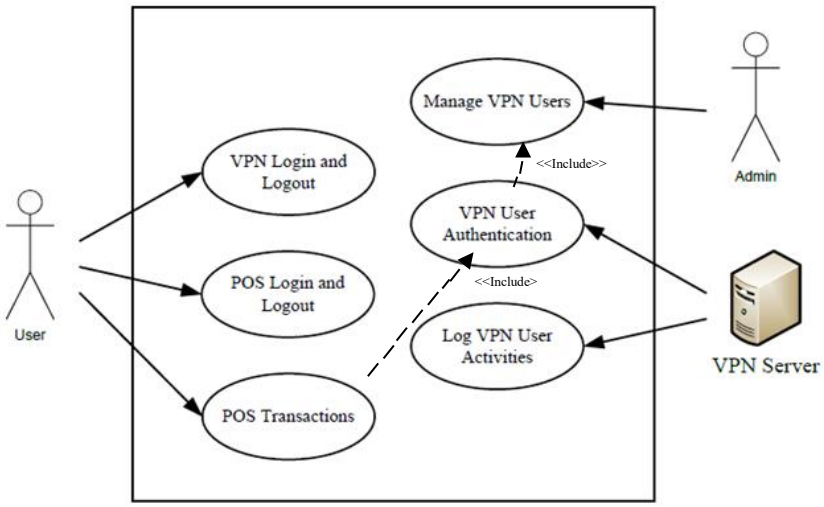

Figure 1. System Use Case Diagram

The oversight of VPN users entailed the addition of accounts and their corresponding credentials. These credentials were essential for logging into the VPN server before gaining access to the POS server. Once authenticated by the VPN server, users were granted access to the POS server. To log in and out of the POS server, users were required to utilize their credentials specific to the POS server. Following a successful login, users could proceed with POS transactions. Notably, the VPN authenticated user credentials and certificates during the VPN login, representing a high level of security for system access. All user activities were meticulously logged by the VPN server and captured using the Wireshark application. The system was composed of three activity diagrams, namely the VPN user management, the POS server to VPN server connection process, and the user to POS server connection process.

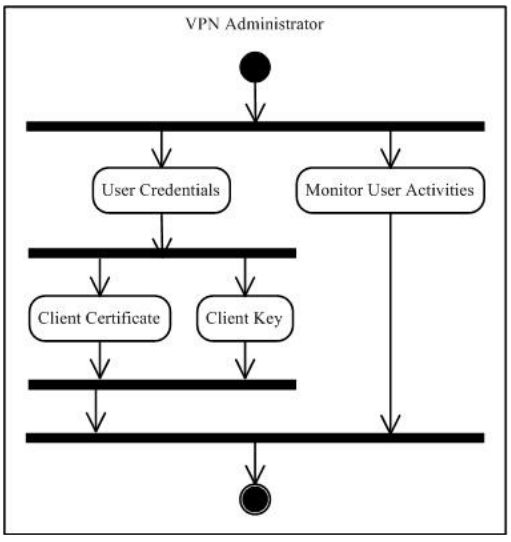

Figure 2. VPN User Management

In the Figure 2, the duties of the VPN administrator encompassed the addition of users and the oversight of their activities. During the user addition process, the administrator was required to collect pertinent credentials, including usernames and passwords. Utilizing this

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

information, the VPN server generated client certificates and keys, with each client receiving a unique client key. Subsequently, the client certificate and key were integrated into the Open VPN application of the VPN. Notably, both the POS server and POS client were categorized as VPN clients. In addition to the certificate and key generation tasks, the administrator assumed the responsibility of monitoring user activities via their respective logs. These logs were accessible for viewing using the Wireshark application.

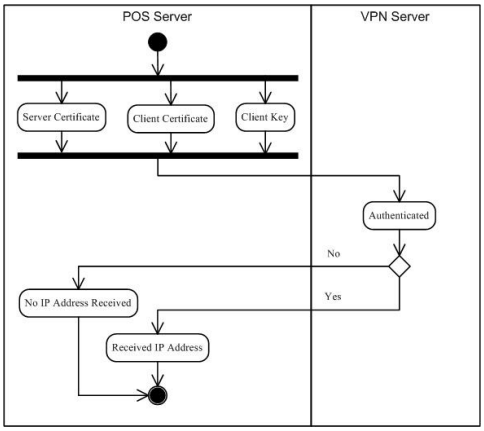

Figure 3. POS Server to the VPN Server Connection Process

Figure 3 depicted the step-by-step process of establishing the connection between the POS server and the VPN server. The sequence began with the requirement that the POS server be connected prior to the user attempting to connect to the POS server. Failure to establish this initial connection rendered the POS inaccessible to all POS clients. Upon initiating the connection to the VPN server, the POS server was mandated to furnish the VPN server certificate, client certificate, and client key. Notably, the server certificate was generated by the VPN server. The VPN server then undertook the authentication of the POS server, accomplished by cross-referencing the security certificates and the key. If these components aligned, the VPN server granted the POS server an Internet Protocol (IP) address. In the absence of a match, no IP address was provided. The detailed steps of this process were effectively captured in the activity diagram shown below.

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

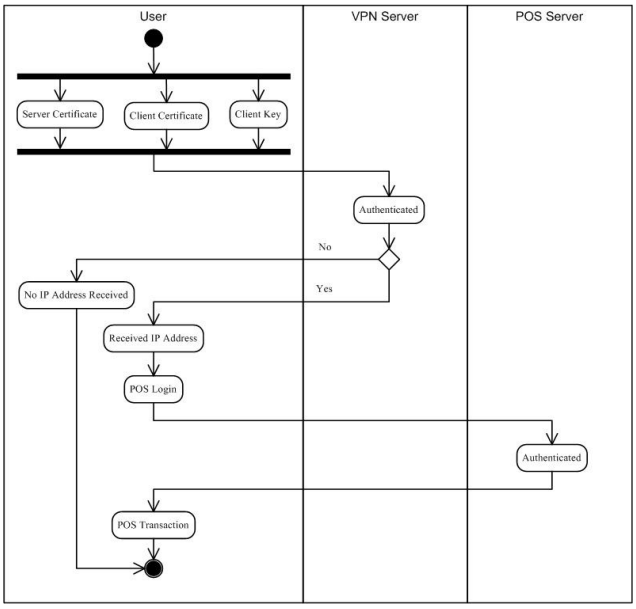

Figure 4. User to POS Server Connection Process

For the user to connect to the POS server, the initial step required connecting to the VPN server. The authentication process mirrored the procedure by which the POS server connected to the VPN server. The VPN server mandated that the user provide the appropriate certificates and key. Upon successful authentication by the VPN server, the user gained access to the POS server. At this stage, the user's credentials for POS login necessitated the use of the username and password specific to the POS server. Following a successful login, the user could then engage in various POS transactions.

System architecture was a crucial aspect, encompassing the architectural design, concept model, and behavior of the proposed technology. It served as a formal and descriptive representation of the technology, organized to facilitate reasoning about the structures and behavior of the overall system. This section entailed an extensive description of the system components that augmented the developed system, contributing to the implementation of the POS over VPN for the USLS Bookstore.

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

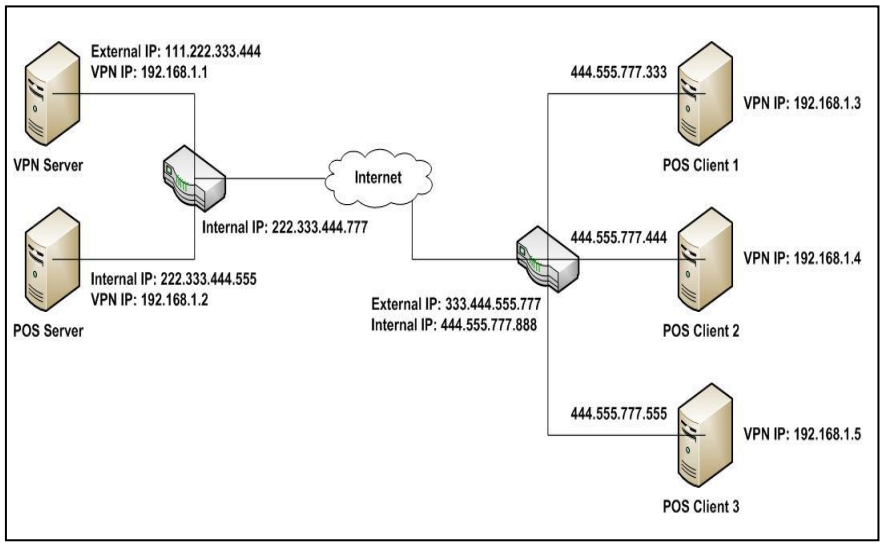

Figure 5. System Architecture of POS over VPN on USLS Bookstore

Moreover, the VPN architecture enabled the user and the system to collaborate effectively, accomplishing the set objectives of the system. This illustrated the crucial significance of the system design to the end-users by employing system architecture concepts and behavior. The communication between the main servers and the VPN remained consistently robust owing to the high level of security embedded in data processing and transactions. The three computer units designated for the administrator, inventory, and cashier were all meticulously authenticated through their respective user-level security protocols. All data was channeled through the main server to ensure data protection, consistency, and overall data efficiency. The cashier, responsible for handling the front-end operations, including order acceptance and receipt generation, contributed to the seamless functioning of the entire system.

Software specifications

Software specifications were meticulously considered by the researchers, outlining the specific requirements for both the server and the client. These specifications included the operating system, VPN services and applications, server services for security, as well as the LAMP server services. The detailed specifications of the server and the client are outlined in the table 2 below.

Table 2. Software specifications server and client.

Server	Client
Centos 7 OS 64-Bit Server	Windows 8 OS
VPN Services and Applications	Open VPN Application
IP Tables or Firewall Services (for securing the external access shutdown)	Visual Foxpro
LAMP Services Server	

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Hardware specifications

The hardware required for the Virtual Private Network (VPN) implementation in the USLS Bookstore included the VPN server, client, and network implementations. In assessing the VPN server and clients, the researchers considered various components such as the processor, motherboard, memory, hard drive, local area network (LAN) interfacing card, and the power supply. Additionally, for the network infrastructure, the specifications of the switch, cable, and bandwidth were thoroughly examined. It is worth noting that the brand or name of the switch was not included in the specifications. The detailed specifications of the VPN server and client are presented in the table 3 below.

Table 3. Hardware specifications of the VNP server and client.

Component	Server Specification	Client Specification
Processor	Intel Xeon E52699A-V4, 55 MB Cache 22 Cores, 44 Threads 3.60 GHz	Intel Quad Core 2.4 GHz L2 Cache
Motherboard	Intel Xeon ES-1200 V3 Series	P5KPL-AM
Memory	8 GB 4x DIMM Series	2 GB
Hard Drive	3000 GB 7.2 RPM SATA Enterprise	500 GB
LAN Card	2x 1GB Integrated LAN	1 GB Integrated LAN
Power Supply	800 Watts	400 Watts

The table 4 below displayed the components specifications required by the Virtual Private Network (VPN) implementation.

Table 4. Network cable and bandwidth specification.

Component	Specification
Cables	UTP CAT 5e or 6 RJ-45
Bandwidth	5 MB of any Telecommunications Providers (Routers and configurations are included)
Memory and Processor	ARM9E @ 800 MHz 128 Flash
Packet Buffer Size	1.5 MB Dynamically Allocated, 256 MB DDR3

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Ports	4 Fiber Ports 24 Autosensing 10/100 Ports (IEEE 802.3 Type 10 Base-T, IEE 802.3µ Type 100 Base-TX) Media Type: Auto-MDIX Half or Full Duplex 2 Dual-Personality Ports
Management	Intelligent Management Center(IMC) Command-Line Interface (CLI) Configuration Menu Out-of-Band Management (Serial RS-232C or Micro-USB) IEEE 802.3 Ethernet MIB Repeater MIB Ethernet Interface MIB

System Implementation

During the implementation of the design, all hardware and software requirements were carefully considered. The server was hosted in the data center of the Information Technology Services (ITS) office. To ensure the ongoing maintenance of the server and clients, the responsibility was assigned to the network services staff. Additionally, the researchers conducted comprehensive training sessions for both the server and client sides. The business analysts who provided support for the Point-of-Sale (POS) system of the bookstore were also trained on the client side.

On the server side, credentials were added for each client for Virtual Private Network (VPN) authentication. After successful authentication, the client was able to connect to the Internet Protocol (IP) address of the POS server. A shared folder with read and write permissions was made accessible to all the clients. This shared folder contained the existing POS system of the bookstore. To safeguard against data loss, an automatic backup script provided by the business analyst was implemented. This script was designed to ensure that all data remained updated during transactions and could recover any deleted files.

System Testing

During the system testing phase, the researchers conducted tests on the Point-of-Sale (POS) system, both with and without the use of the Virtual Private Network (VPN) server. In the absence of the VPN, the researchers utilized the credentials of the user from the POS server. This entailed connecting two POS clients to the POS server in the Local Area Network (LAN) and recording the duration of the client's connection to the server. Subsequently, when testing the POS using the VPN server, the researchers received support from the business analyst of the Information Technology Services (ITS), who also functioned as the programmer of the POS system and the POS administrator. In this scenario, an additional computer was added by the researchers to act as the VPN server. Throughout the test, the researchers documented the duration of the client's connection to the server as well as the user logs. The Wireshark application was used for the analysis of the logs. Notably, when using the VPN server, the researchers ensured that the POS server was connected before the user logged in to the VPN server.

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Deployment

For the deployment of the system, the researchers sought permission from the director of the Information Technology Services (ITS) to host the server in their data center. Maintenance was carried out by the researchers for one year, after which it was transitioned to the network support services staff. For the bookstore, the OpenVPN application was installed for each client to enable connection to the VPN server and access to the Point-of-Sale (POS) server.

3. Results and Discussion

The first objective of the study was to determine the VPN policy framework to be included in the areas of scope and binding, authentication method, and VPN credentials and protocols. Concerning the system's scope and binding, the researchers installed the application Fail2Ban to safeguard the VPN server from potential malicious attacks, such as distributed denial-of-service (DDoS) attacks, which aim to disrupt the server's normal traffic (Cloudflare, Inc., 2019). This application was established as a service, enabling the server to respond to any unauthorized access resulting from a DDoS attack. The secure logs of the VPN server, where Fail2Ban was initiated as a service, are presented below.

Apr 16 12:05:18 VpnServer sshd[1278]: Failed password for invalid user minecraft from 142.93.210.145 port 44434 ssh2
Apr 16 12:05:19 VpnServer sshd[1270]: Failed password for invalid user minecraft from 80.52.199.93 port 34978 ssh2
Apr 16 12:05:33 VpnServer sshd[1290]: Failed password for invalid user minecraft from 36.89.157.197 port 34856 ssh2
Apr 16 12:12:02 VpnServer sshd[1523]: Failed password for invalid user vagrant from 51.77.201.36 port 37332 ssh2
Apr 16 12:16:34 VpnServer sshd[1609]: Failed password for invalid user miguel from 51.77.201.36 port 53644 ssh2
Apr 16 12:21:46 VpnServer sshd[1730]: Failed password for invalid user helpdesk from 222.110.45.23 port 46688 ssh2
Apr 16 12:26:35 VpnServer sshd[1805]: Failed password for invalid user andrea from 174.138.57.147 port 56090 ssh2
Apr 16 12:26:47 VpnServer sshd[1813]: Failed password for invalid user csgo from 222.110.45.23 port 34744 ssh2
Apr 16 12:32:59 VpnServer sshd[1946]: Failed password for invalid user dh from 206.189.165.94 port 40062 ssh2
Apr 16 12:33:47 VpnServer sshd[1956]: Failed password for invalid user ibmadrc from 92.50.249.166 port 50042 ssh2
Apr 16 12:37:22 VpnServer sshd[2013]: Failed password for invalid user mo from 206.189.165.94 port 56304 ssh2
Apr 16 12:38:29 VpnServer sshd[2037]: Failed password for invalid user Senja from 92.50.249.166 port 37408 ssh2
Apr 16 12:43:38 VpnServer sshd[2146]: Failed password for invalid user ftpnew from 188.165.206.185 port 57598 ssh2
Apr 16 12:48:14 VpnServer sshd[2220]: Failed password for invalid user uftp from 188.165.206.185 port 45266 ssh2

Apr 16 13:02:54 VpnServer sshd[2518]: Failed password for invalid user sabrina from 208.114.112.169 port 50742 ssh2
Apr 16 13:02:59 VpnServer sshd[2529]: Failed password for invalid user ts3 from 80.211.169.69 port 51212 ssh2
Apr 16 13:06:22 VpnServer sshd[2579]: Failed password for invalid user pagar from 130.211.184.153 port 46694 ssh2
Apr 16 13:07:06 VpnServer sshd[2596]: Failed password for invalid user uucp from 208.114.112.169 port 42752 ssh2
Apr 16 13:08:20 VpnServer sshd[2617]: Failed password for invalid user stress from 80.211.169.69 port 39014 ssh2
Apr 16 13:11:14 VpnServer sshd[2690]: Failed password for invalid user admin from 130.211.184.153 port 34890 ssh2
Apr 16 13:12:07 VpnServer sshd[2714]: Failed password for invalid user princesa from 198.98.53.45 port 42902 ssh2
Apr 16 13:12:23 VpnServer sshd[2718]: Failed password for invalid user princesa from 178.203.119.130 port 47324 ssh2
Apr 16 13:15:42 VpnServer sshd[2779]: Failed password for invalid user admin from 110.19.68.56 port 33329 ssh2
Apr 16 13:15:44 VpnServer sshd[2779]: Failed password for invalid user admin from 110.19.68.56 port 33329 ssh2
Apr 16 13:15:47 VpnServer sshd[2779]: Failed password for invalid user admin from 110.19.68.56 port 33329 ssh2
Apr 16 13:15:49 VpnServer sshd[2779]: Failed password for invalid user admin from 110.19.68.56 port 33329 ssh2
Apr 16 13:16:30 VpnServer sshd[2793]: Failed password for invalid user ce from 198.98.53.45 port 36937 ssh2
Apr 16 13:17:46 VpnServer sshd[2821]: Failed password for invalid user ce from 178.203.119.130 port 35632 ssh2
Apr 16 13:18:29 VpnServer sshd[2835]: Failed password for invalid user tgz from 58.87.72.113 port 57198 ssh2
Apr 16 13:26:21 VpnServer sshd[2982]: Failed password for mysql from 58.87.72.113 port 43030 ssh2
Apr 16 13:46:35 VpnServer sshd[3348]: Failed password for invalid user hi from 178.124.189.122 port 48167 ssh2
Apr 16 13:49:50 VpnServer sshd[3404]: Failed password for invalid user eu from 68.183.124.53 port 59452 ssh2
Apr 16 13:50:42 VpnServer sshd[3445]: Failed password for invalid user sg from 202.103.37.40 port 43998 ssh2
Apr 16 13:52:06 VpnServer sshd[3528]: Failed password for invalid user nvidia from 193.188.22.12 port 32530 ssh2
Apr 16 13:52:11 VpnServer sshd[3530]: Failed password for invalid user test from 193.188.22.12 port 35893 ssh2
Apr 16 13:53:59 VpnServer sshd[3567]: Failed password for invalid user git from 68.183.124.53 port 47448 ssh2
Apr 16 13:54:34 VpnServer sshd[3575]: Failed password for invalid user yy from 178.124.189.122 port 42404 ssh2

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Apr 16 13:56:43 VpnServer sshd[3629]: Failed password for invalid user ahziasa from 202.103.37.40 port 59426 ssh2
Apr 16 13:56:43 VpnServer sshd[3627]: Failed password for apache from 223.93.172.151 port 38337 ssh2

Based on the recorded results generated by the VPN server, there were 37 attempts with a failed password for an invalid user and two attempts with a failed password for a valid user. The logs also provided information regarding the IP address from which the attack originated, the port that was utilized, and the name of the user. Alongside this log, the firewall documented all the IP addresses that were blocked, originating from where the attack was launched. The content of the firewall logs is presented below.

-A f2b-sshd -s 5.135.214.166/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 5.135.135.116/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 37.187.23.116/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 220.119.171.121/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 219.142.28.206/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 218.92.0.207/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 218.92.0.175/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 218.92.0.154/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 218.92.0.140/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 210.13.102.89/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 195.231.8.94/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 189.3.152.194/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 182.72.104.106/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 177.94.224.157/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 177.131.122.210/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 173.167.200.227/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 165.227.39.71/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 165.227.150.158/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 150.109.51.205/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 144.217.4.14/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 142.93.50.178/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 138.219.192.98/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 128.91.208.83/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 128.199.71.167/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 122.192.33.102/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 120.92.209.112/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 119.40.53.50/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 118.25.210.180/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 114.67.228.87/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 111.75.205.166/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 107.170.73.105/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 106.51.154.30/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 104.198.93.19/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 103.36.84.100/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 103.113.105.11/32 -j REJECT --reject-with icmp-port-unreachable

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

-A f2b-sshd -s 101.251.197.238/32 -j REJECT --reject-with icmp-port-unreachable
-A f2b-sshd -s 181.48.116.50/32 -j REJECT --reject-with icmp-port-unreachable

In the VPN authentication method, the researchers initially generated the server certificate authority, key, and encryption files. For the encryption algorithm, a public-key cryptography protocol known as Diffie-Hellman was utilized. This protocol enables two parties to establish a shared key over an insecure communication channel (Mishra and Kar, 2017). Additionally, client certificate and key files were created for the client. The certificates and keys generated for both the server and client are presented in Table 5 below.

Table 5. Certificate and key files generation.

User	Terminal Command	Generated Certificate and Key Files
root (VPN server)	build-key-server	server.crt server.key
test1 (VPN client 1)	build-key test1	test1.crt test1.key
test2 (VPN client 2)	build-key test3	test2.crt test2.key
test3 (VPN client 3)	build-key test3	test3.crt tes3.key

In the VPN client side, the OpenVPN application configuration files contained the server security certificate, user security certificate, and user key, which were added to the config folder of the Open VPN application. For client 1, which served as the POS server, the files that were copied included server.crt, test1.crt, and test1.key. For client 2, the files that were copied were server.crt, test2.crt, and test2.key, while for client 3, they were server.crt, test3.crt, and test3.key. During the process of connecting client 1 to the server, these files were authenticated by the server. Following the authentication, the server provided an IP address for that client, and the Open VPN icon turned green to indicate a successful connection. To ensure data privacy, the actual public IP address and port of the VPN firewall were replaced with "Firewall IP:port_n" when presenting the logs during the authentication process.

The table 6 below presents the IP addresses provided by the server after the users were authenticated.

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Table 6. IP addresses provided by the server after authentication.

User	VPN Server Log	IP Address
test1	Fri Jan 18 18:10:19 2019 Firewall IP:port[test1] Peer Connection Initiated with [AF_INET] Firewall IP:port_1 Fri Jan 18 18:10:19 2019 test1/ Firewall IP:port_1 MULTI_sva: pool returned IPv4=192.168.1.34, IPv6=(Not enabled) Fri Jan 18 18:10:19 2019 test1/ Firewall IP:port_1 MULTI: Learn: 192.168.1.34 -> test1/ Firewall IP:port_1 Fri Jan 18 18:10:19 2019 test1/ Firewall IP:port_1 MULTI: primary virtual IP for test1/ Firewall IP:port_1: 192.168.1.34	192.168.1.34
test2	Fri Jan 18 18:10:04 2019 test2 Firewall IP:port_2 MULTI_sva: pool returned IPv4=192.168.1.38, IPv6=(Not enabled) Fri Jan 18 18:10:04 2019 test2/ Firewall IP:port_2 MULTI: Learn: 192.168.1.38 -> test2/ Firewall IP:port_2 Fri Jan 18 18:10:04 2019 test2/ Firewall IP:port_1_2 MULTI: primary virtual IP for test2/ Firewall IP:port_2: 192.168.1.38	192.168.1.38
test3	Fri Jan 18 18:10:12 2019 test3/ Firewall IP:port_2 MULTI_sva: pool returned IPv4=192.168.1.42, IPv6=(Not enabled) Fri Jan 18 18:10:12 2019 test3/ Firewall IP:port _3 MULTI: Learn: 192.168.1.42 -> test3/ Firewall IP:port_3 Fri Jan 18 18:10:12 2019 test3/ Firewall IP:port_3 MULTI: primary virtual IP for test3/ Firewall IP:port_3: 192.168.1.42	192.168.1.42

The users were successfully authenticated by the server and provided with the primary virtual IP addresses 192.168.1.34, 192.168.1.38, and 192.168.1.42 for test1, test2, and test3, respectively. Subsequent lines in the logs indicated that the connection was established with the message "TCP connection established with [AF_INET]Firewall IP:port.”.

The VPN credentials involved in the system were the server certificate, client certificate, and client key files. For the VPN protocol, the researchers opted to use the transport control protocol (TCP) instead of the user datagram protocol (UDP). The VPN protocol employed a security protocol that utilized SSL/TLS for the key exchange, ensuring secure connections using the point-to-point tunneling protocol or PPTP (VPN Unlimited).

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Table 7. Evaluation of Quality of VPN

Criteria of Evaluation	Mean	Interpretation
Scalability	4.50	Excellent
Efficiency	4.00	Very Good
Effectiveness in Authentication and Security	3.75	Very Good
Average	**4.08**	**Excellent**

Regarding the evaluation of the effectiveness in terms of authentication and security quality of Virtual Private Networks (VPNs), the configuration of the Apache evasive module of the Apache web server was not included. This decision was made due to the focus solely on the Fail2Ban security prevention in the VPN Server.

Quality of VPN

In the pursuit of the second objective of the study, the examination of VPN quality focused on evaluating the scalability, efficiency, and effectiveness in terms of authentication and security. For scalability, the server was configured to accommodate up to 100 users, as specified in the file named server.conf.

```
# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 100
```

Although the system was designed to support 100 users, a scalability test was conducted with only 11 clients for testing purposes. Of these 11 clients, 3 were tested in the ITS office, while the remaining 8 were tested in the computer research laboratory.

Table 8. List of clients that are concurrently connected to the server.

Computer	User	IP Address Provided
Computer 1	test1	192.168.1.34
Computer 2	test2	192.168.1.38
Computer 3	test3	192.168.1.42
Computer 4	test4	192.168.1.46
Computer 5	test5	192.168.1.54
Computer 6	test6	192.168.1.50
Computer 7	test7	192.168.1.58
Computer 8	test8	192.168.1.62
Computer 9	test9	192.168.1.66
Computer 10	test10	192.168.1.70
Computer 11	test11	192.168.1.74

To record the packets between the VPN clients and the VPN server, the researchers utilized the Wireshark application. Below are the detailed packets for the three (3) clients and the POS transactions of user test 3.

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

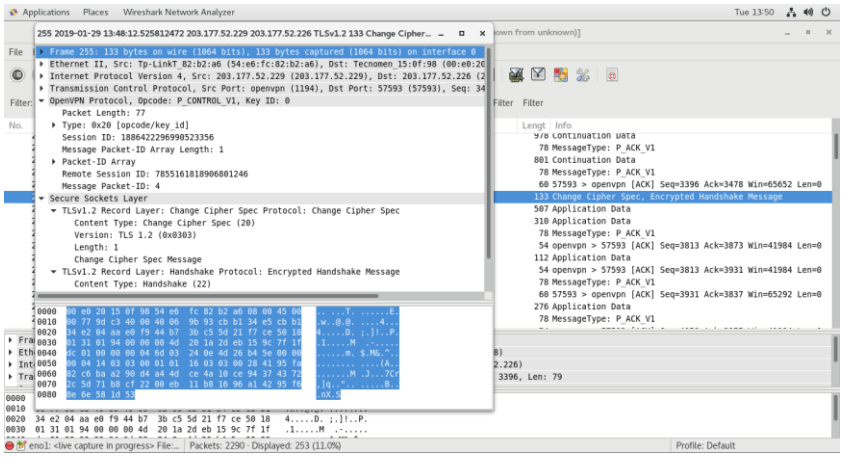

Figure 6. Packets of test1 User

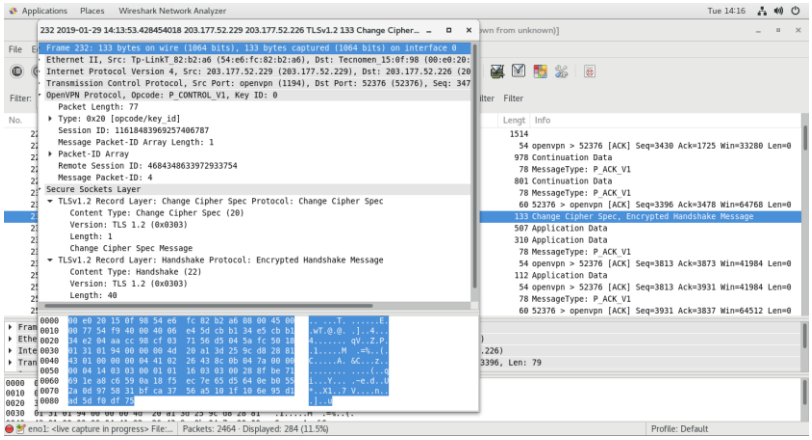

Figure 7. Packets of test2 User

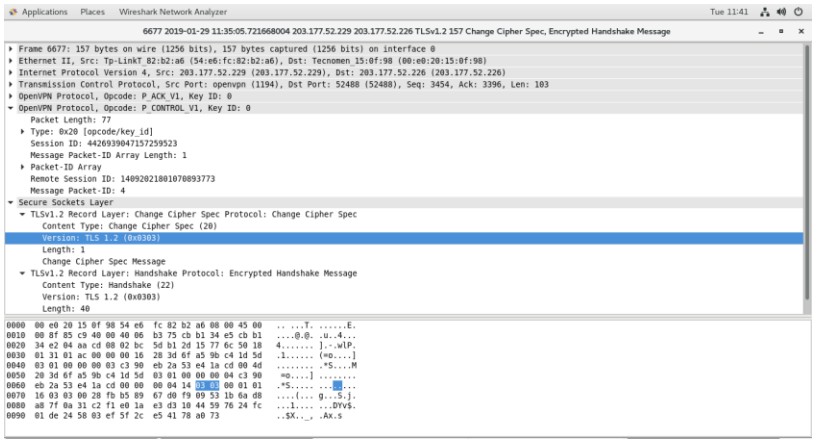

Figure 8. Packets of test3 User

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

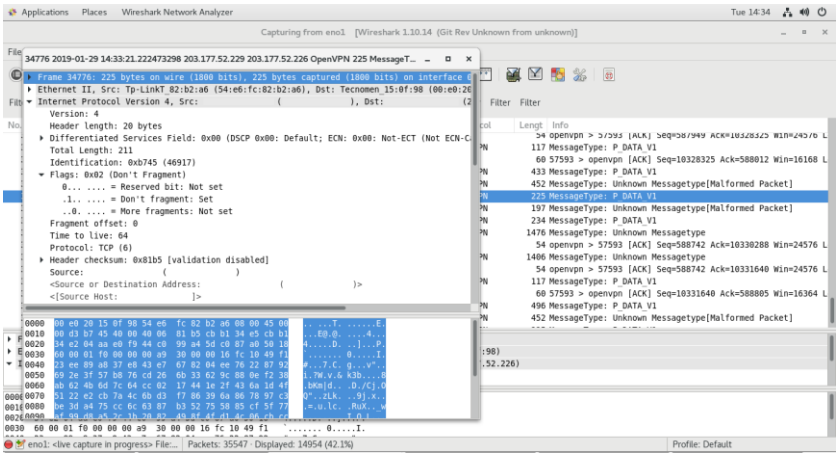

Figure 9. POS Transaction Packet

The installation of the POS system for the bookstore was previously carried out remotely using the TeamViewer application. In this process, the administrator remotely connected to the POS client and copied the POS application files. It was assumed that the client already had the TeamViewer and Visual FoxPro application installed. Consequently, whenever a new POS client was added, the administrator remotely copied the POS application files. With the introduction of the VPN, a dedicated POS server eliminated the need to install the POS application files on the client side. Instead, all clients were required to install the OpenVPN application to connect to the VPN server. After successful authentication, the POS application folder was shared and the application was executed. Although all clients shared the same folder, each client had their respective POS user accounts, ensuring that each user accessed their own database. Consequently, the database of one client did not overlap with that of another. As the system was equipped with its own POS server, the administrator consolidated the inventory of all the clients on the server. Without the VPN implementation, the administrator would have remotely copied all client databases via the TeamViewer application to consolidate them.

The effectiveness of the VPN server's security against DDoS attacks was determined by the Fail2Ban application. DDoS attacks were typically orchestrated using a zombie network, where computers in the network were infected with denial-of-service (DOS) attacking tools. Hackers utilized these infected computers to launch attacks on the server, rendering it unavailable to legitimate users and potentially bringing the service down. According to the server and firewall logs, all randomly generated users failed in their attempts to attack the server. Only two generated users, namely mysql and apache, were valid, while the remaining users were deemed invalid. The firewall rejected all IP addresses from which the attacks originated.

Regarding the effectiveness of VPN user authentication, the researchers conducted tests using only the user "test1." The required files to be copied to the VPN client were "server.ca," "test1.crt," and "test1.key." The tests considered various scenarios, such as deleted or missing files or the use of certificate or key files belonging to a user other than "test1." In all test scenarios, the user "test1" was unable to connect to the server. The table 9 below presents the test results and the recorded logs by the client.

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Table 9. Effectiveness in user authentication.

Certificate and Key Files	Logs	Remarks
test1.crt, test1.key and no server.ca	Options error: --ca fails with 'ca.crt': No such file or directory (errno=2)	test1 was not connected to the VPN server
test1.key, server.ca and no test1.crt	Options error: --cert fails with 'test1.crt': No such file or directory (errno=2)	test1 was not connected to the VPN server
server.ca, test1.crt and no server.ca	Thu Apr 18 11:13:46 2019 WARNING: cannot stat file 'test1.key': No such file or directory (errno=2) Options error: --key fails with 'test1.key' Thu Apr 18 11:16:50 2019 WARNING: cannot stat file 'test1.key': No such file or directory (errno=2) Options error: --key fails with 'test1.key'	test1 was not connected to the VPN server
test1.crt, test1.key and server.ca was renamed	Options error: --ca fails with 'ca.crt': No such file or directory (errno=2)	test1 was not connected to the VPN server
server.ca, test1.crt and test2.key	Thu Apr 18 11:09:06 2019 WARNING: cannot stat file 'test1.key': No such file or directory (errno=2) Options error: --key fails with 'test1.key'	test1 was not connected to the VPN server
server.ca, test2.crt, test1.key	Options error: --cert fails with 'test1.crt': No such file or directory (errno=2)	test1 was not connected to the VPN server

For evaluating the effectiveness of the VPN server concerning packet transmission, the POSmain_new.FXP module was utilized to capture the packets. In this process, the researchers logged into the POS application, assuming that no VPN server was installed in the network. The captured packet contained the name of the module, as indicated below:

Eximia Journal
Vol. 12, 570-589, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

.x.....p.o.s.m.a.i.n._.n.e.w...F.X.P.....MxAc.....SMB@.....
.J.....Y.....'e.....'e.....Up....~9..%....0.....!.....
.....

The same module was employed by the researchers; however, this time the VPN server was installed, and the researchers logged in to the VPN server before logging in to the POS application. In the captured packets, the name of the module was not indicated.

Table 10. Evaluation of VPN Framework

Criteria of Evaluation	Mean	Interpretation
Scope and Binding in terms of DDos attack	4.50	Excellent
Authentication Methods	4.00	Very Good
VPN Credentials and Security Protocols	4.50	Excellent
Average	**4.33**	**Excellent**

In the evaluation of virtual private networks concerning authentication methods, it did not include the revoking of users' accounts, where the deleted users had a certificate embedded in their accounts. Therefore, it was necessary to revoke it manually to disable their authentication at the server, preventing them from logging in if their account was revoked.

4. Conclusion ad Recommendations

The VPN policy framework of this study included the areas of scope and binding, authentication method, and VPN credentials and protocols. In the scope and binding, all DDoS attacks were rejected by the firewall using the Fail2Ban application. Before the user was granted access to the POS server, the user had to connect to the VPN server, which required the server certificate authority file, the user certificate, and key files. These files were then copied to the VPN client. If a user was created in the VPN server, their certificate and key files were also generated. After a successful login to the VPN server, an IP address was provided by the server to the user. The protocol used in this system was TCP instead of UDP. For the framework, the use of the Fail2Ban application successfully rejected all malicious attacks that could deny service to the legitimate users or even shut down the server. The authentication method was needed to authenticate the user in connecting to the VPN server. The TCP protocol was a secure protocol that utilized SSL/TLS for key exchange.

The level of VPN quality was in terms of scalability, efficiency, and effectiveness. The total number of clients that could be accommodated by the VPN server was configured in the server.conf file. A total of 11 users were created, and all of them were successfully connected to the server. For the POS clients, a shared folder was provided instead of manually installing the POS application to each client using the TeamViewer. With the presence of the VPN server, the steps in the addition of a new POS client were reduced. During the authentication process, the server certificate authority, user certificate, and key files had to be copied to the client. The user could not connect to the server if there was an alteration of at least one of these or if some files were missing. Logs were being recorded in the VPN client if the user could not connect to the server if the credentials were not authenticated by the server. With the VPN server, the packets from the client were encrypted, and the name of the application could not be seen in plain text. Unlike if there was no VPN server, the name of the application was not encrypted in the packets. The system was scalable in terms of the number of clients by defining the value of

the parameter max-clients in server.conf. Server and user credentials were an effective method used during the authentication process. All packets that were transmitted by the VPN client to the VPN server were encrypted, which was one way to secure the user's data. The user authentication method was effective in verifying if the user was legitimate.

For further study, the researchers recommend that the mod_evasive Apache module be installed in the VPN server. This module would protect the server against DoS, DDoS, and brute force attacks on the Apache server (Garais and Enaceanu, 2016). If the server was being attacked, the module would report abuses through email and the syslog facilities. In case the server was attacked, a 403 response would be sent, and the IP address would be logged. This IP address could be blocked using a system command.

In the evaluation of authentication, the researchers would include scripts that would run to automate the revoking of the users and their certificates after they resigned or were kicked out of a certain company. This configuration would lessen the work of the server administrator in their tasks for monitoring.

References:

[1] Borky JM, Bradley TH (2018). Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering. 2018 Sep 9:345–404. doi: 10.1007/978-3-319-95669-5_10. PMCID: PMC7122347.

[2] Cloudflare, Inc. (2019). What is a DDoS attack? Retrieved from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[3] Garais, Gabriel Eugen, and Alexandru-Serban Enaceanu (2016). "Open source servers and website platforms security." Journal of Information Systems & Operations Management, vol. 10, no. 2, Dec. 2016, pp. 503+. Gale Academic OneFile, link.gale.com/apps/doc/A483829378/AONE?u=googlescholar&sid=bookmark-AONE&xid=9e917cde. Accessed 13 Dec. 2023.

[4] Iqbal, Muhammad & Riadi, Imam. (2019). Analysis of Security Virtual Private Network (VPN) Using OpenVPN. International Journal of Cyber-Security and Digital Forensics. 8. 58-65. 10.17781/P002557.

[5] Jeremy Faircloth, J. (2017). Chapter 9 - Wireless penetration testing, Penetration Tester's Open Source Toolkit (Fourth Edition), Syngress, Pages 319-369, ISBN 9780128021491, https://doi.org/10.1016/B978-0-12-802149-1.00009-9.

[6] Karaymeh, Ashraf & Ababneh, Mohammad & Qasaimeh, Malik & Al-Fayoumi, Mustafa. (2019). Enhancing Data Protection Provided by VPN Connections over Open WiFi Networks. 1-6. 10.1109/ICTCS.2019.8923104.

[7] Mardisalu, R. (2019, February 26). VPN beginner’s guide. Retrieved from https://thebestvpn.com/what-is-vpn-beginners-guide/

[8] Mishra, Manoj & Kar, Jayaprakash. (2017). A study on diffie-hellman key exchange protocols. International Journal of Pure and Apllied Mathematics. 114. 10.12732/ijpam.v114i2.2.

[9] Prasad, S., Nagle, M., & Khan, T. Z. (2016). Preventation of Data Content Leakage with Secured Encryption Algorithm. IJARCCE, 5(12), 295–297. https://doi.org/10.17148/IJARCCE.2016.51267

[10] Xiong, Andre (2019). College Students' Perceptions and Usage of Virtual Private Networks. http://arks.princeton.edu/ark:/88435/dsp01v979v5902