Library Progress International *Print version ISSN 0970 1052*
Vol.44 No. 3, Jul-Dec 2024: P. 17006-17020 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

A Comparative Analysis of VPN and Proxy Protocols in Library Network Management

Balachandran, S.[1*], Dominic, J.[2,] and Sivankalai, S.[3]

[1*]Research Scholar, Hindustan Institute of Technology and Science, Padur, Chennai–603103. Tamil Nadu, India itsbaala@gmail.com, 0000-0002-5893-1604
[2]Chief Librarian, Hindustan Institute of Technology and Science, Padur, Chennai–603103. Tamil Nadu, India Jdom16@gmail.com, 0000-0002-6039-641X
[3]Assistant University Librarian, Anna University, Chennai–600025 Tamil Nadu, India skysivan@gmail.com, *0000-0002-1174-7594*

How to cite this article: Balachandran, S.*, Dominic, J., and Sivankalai, S. (2024) A Comparative Analysis of VPN and Proxy Protocols in Library Network Management. *Library Progress International,* 44(3), 17006-17020

Abstract
In the rapidly evolving digital environment, libraries and similar institutions are increasingly reliant on advanced network technologies to manage and secure access to their extensive digital resources. This study examines two prominent technologies Virtual Private Networks (VPNs) and proxy servers focusing on their performance in handling substantial data volumes and their respective advantages in terms of security and efficiency. VPNs offer a secure, encrypted connection that masks the user's IP address and protects data from cyber threats, making them ideal for safeguarding sensitive information and ensuring secure remote access to digital resources. Conversely, proxy servers act as intermediaries, improving privacy, circumventing geographical restrictions, and enhancing performance through caching. This research provides a comparative analysis of VPN and proxy services by simulating typical file transfer scenarios and assessing key network metrics, including packet handling, byte throughput, and transfer times. The study aims to highlight the strengths and weaknesses of each technology in various conditions and their impact on network performance. The findings offer valuable insights for libraries and institutions seeking to optimize their network infrastructure, aiding them in making informed decisions about which technology best meets their needs for security, efficiency, and data management. By understanding the relative performance of VPNs and proxies, organizations can develop more effective and secure network strategies, enhancing their ability to provide reliable access to digital resources in an increasingly complex digital landscape.

Keywords: VPN, Proxy, Packet, Security, I/O Graph, Network Management, Traffic Patterns

Introduction

In today's digital era, libraries and similar institutions increasingly rely on advanced network technologies to efficiently manage and disseminate information. With the rapid expansion of digital resources, secure and effective access has become essential, prompting libraries to adopt sophisticated solutions like VPN and proxy servers. Both technologies are critical for managing internet access, enhancing security, and ensuring privacy, but they operate through different mechanisms and offer distinct advantages. VPNs establish secure, encrypted connections between a user's device and a remote server, masking the user's IP address and protecting internet traffic from unauthorized interception (Huang & Frahim, 2008). This encryption safeguards sensitive information, making VPNs invaluable for libraries that provide remote access to digital resources such as academic journals, databases, and e-books (Balachandran & Dominic, 2023). By encrypting all data traffic, VPNs ensure that libraries' sensitive information is protected from cyber threats, enabling secure access from any location (Newman, 2009). Conversely, proxy servers act as intermediaries between users and the internet, forwarding requests and responses through the proxy, thereby enhancing privacy, bypassing geographical restrictions, and improving performance through caching (Abrams et al., 1995). Proxies are especially beneficial for libraries that need to control internet usage, monitor web traffic, or restrict access to specific sites (Covey, 2003).

The decision to employ VPNs or proxies largely depends on the specific needs and objectives of the organization. VPNs are ideal for robust security and privacy, particularly for protecting sensitive data and securing remote access (Kose et al.,

2024; Miracle, 2024). On the other hand, proxies provide greater flexibility in managing internet traffic, improving performance, and implementing content filtering (Rus et al., 2024). As libraries face increasing cybersecurity threats, evaluating their network security and access strategies is essential. Both VPNs and proxies offer unique benefits, and their performance can vary depending on factors like data volume, network load, and traffic types. This study aims to provide a comparative analysis of VPN and proxy services, focusing on their performance in managing large data volumes (Xhemajli & Tafa, 2024). Simulating typical file transfer scenarios, the research will highlight the strengths and limitations of each technology. The findings will offer insights into how VPNs and proxies handle different types of traffic and data loads, helping libraries and institutions make informed decisions about which technology best aligns with their security, efficiency, and data management needs (OJO, n.d.; R. Li & Cao, 2024). By thoroughly evaluating the performance of these technologies, libraries can better prepare themselves to meet the demands of the modern digital landscape, balancing security, performance, and privacy in their network strategies.

Literature Review

The performance of VPN and proxy protocols in managing large data transfers has been widely analyzed in existing literature. VPNs are praised for their robust security features, providing encrypted tunnels that safeguard data from potential breaches. However, as noted by various studies, this encryption can lead to increased latency, particularly with large file transfers. While VPNs are highly effective in securing sensitive information, the trade-off is often reduced speed, which can be a limitation in environments requiring rapid data transmission. On the other hand, proxies are favored for their ability to enhance data transfer speeds by forgoing encryption (Harmening, 2025). Proxies are particularly valuable in scenarios where quick access is more critical than data security. However, the absence of encryption in proxies also introduces security vulnerabilities, making them less suitable for environments handling sensitive information (Bhatti et al., 2024).

When comparing VPNs and proxies, researchers emphasize the balance between security and speed. VPNs consistently provide secure performance but may suffer from encryption overhead, while proxies, though faster, offer less protection. Studies also examine the impact of packet sizes, with VPNs tending to standardize packet lengths due to encryption, creating predictable traffic patterns that can lower efficiency in managing large data volumes. In contrast, proxies allow for more flexibility with variable packet lengths, which can be more efficient in certain scenarios (Kovacs, 2024). Focusing on their use in academic institutions such as libraries, research suggests that proxies may be preferable when speed and throughput are critical, while VPNs are indispensable for ensuring data security (Akinsanya et al., 2024). The importance of network analysis tools is underscored in these evaluations, as they help measure key metrics such as transfer speed, latency, and packet loss, which are crucial in selecting the appropriate protocol for real-world applications. Some literature also advocates for a hybrid approach, combining VPNs and proxies to address both security and speed requirements (Kothapalli, 2023; Naidu & Jha, 2023; Radchenko et al., 2024). Such a strategy could offer a balanced solution, meeting institutional needs without compromising on either aspect. Recent advances in VPN technology, such as more efficient encryption algorithms, aim to reduce latency while maintaining robust security (Azwee et al., 2023; Morsli et al., 2024). Likewise, new developments in proxy technologies are focused on improving speed, while providing some level of data protection, though still not as robust as VPNs (Kovacs, 2024; Dikshit et al., 2023; Neto, 2023). Overall, the literature offers a comprehensive review of VPNs and proxies, especially in the context of handling large data transfers. While VPNs excel in security, their lower speed can make them less effective in high-speed data scenarios. Proxies, while faster, lack encryption, posing significant risks in sensitive data environments. Ultimately, the choice between VPN and proxy protocols should be based on the specific needs of the situation, balancing security and performance. Future research and technological innovations may provide more balanced solutions for managing large data transfers effectively.

Methodology

To investigate the performance of VPN (Bringhenti et al., 2024) and proxy protocols (Burnside et al., 2002) in handling substantial data volumes, an 86.1MB file was utilized, representing a typical file transfer activity (Janbeglou & Brownlee, 2016a). This file size was chosen to provide a robust evaluation of each protocol's capacity to manage large data transfers efficiently (Mani et al., 2018). The dataset was downloaded from Google Drive, as analyzed by (Quick & Choo, 2014), ensuring real-world relevance by simulating common file retrieval scenarios. The analysis was conducted using a network analysis monitor (Chapman, 2016) designed to capture detailed statistics regarding the network traffic generated during the file download (Janbeglou & Brownlee, 2016b). This tool is crucial for measuring various network performance parameters

with precision, including transfer speeds, latency, and packet loss (Chapman, 2016). By employing this specialized tool, the study aimed to ensure accurate and reliable data for assessing the performance of VPN and proxy protocols.
The methodology involved several key aspects:

1. Comprehensive Analysis of VPN and Proxy Protocol Performance
2. Comparative Analysis of Network Performance Metrics
3. Packet Lengths Analysis for VPN and Proxy:
4. I/O GRAPH

Comparative Overview of VPN and Proxy Protocols for Library Systems

This methodology provided a thorough assessment of VPN and proxy protocols, highlighting their respective strengths and weaknesses in managing large data transfers and their relevance to library systems.

Comprehensive Analysis of VPN and Proxy Protocol Performance

Protocol Hierarchy refers to the layered structure of network protocols, where each layer is responsible for specific functions and interacts with the layers directly above and below it. This hierarchical model simplifies network design and troubleshooting by compartmentalizing communication processes. VPN create secure, encrypted connections over the internet (Lacković & Tomić, 2017). The VPN protocol's performance was evaluated in terms of packet handling (Mahmmod et al., 2020), byte transfer efficiency and overall bit rate (Qin et al., 2002). Proxies act as intermediaries between the user and the internet, often used to enhance privacy or bypass restrictions (Lawas et al., 2016). The Proxy protocol's performance was assessed similarly, focusing on packet, byte (S. Zhang et al., 2024), and bit rate (Liebl et al., 2007) management during file transfer (Kim et al., 2010). The following Table-1 provides a detailed comparison of the performance metrics for VPN and Proxy protocols across various network protocols. The analysis covers several key performance indicators, including frame efficiency, packet handling, byte transfer, and bit rate. By examining these metrics, we can assess the strengths and limitations of each protocol in managing network traffic.

Table-1: Comprehensive Analysis of VPN and Proxy Protocol Performance

Sl. No.	**Protocol**	**VPN**	**Proxy**	**Difference**	**Explanation**
1	Frame	100.00%	100.00%	0.00%	Both VPN and Proxy perform equally in terms of frame protocol efficiency.
2	Packets	82,333	98,720	16,387	Proxy handles 16,387 more packets than VPN, indicating better packet handling efficiency.
3	Bytes	10,21,93,905	9,40,84,558	-81,09,347	VPN transfers 81,09,347 more bytes than Proxy, suggesting better byte transfer efficiency.
4	Bits/s	63,63,542.60	93,478.94	1,61,00,000.00	VPN achieves a higher bit rate by 1,61,00,000.00 bits/s compared to Proxy, showing better speed.
5	Ethernet	100.00%	100.00%	0.00%	Both VPN and Proxy have the same efficiency for Ethernet.
6	Packets	82,333	98,720	16,387	Proxy handles 16,387 more Ethernet packets than VPN, indicating better handling of Ethernet traffic.
7	Bytes	11,52,662	13,82,080	2,29,418	Proxy transfers 2,29,418 more bytes over Ethernet than VPN, showing better byte efficiency.

8	Bits/s	93,478.94	61,00,032.19	-61,506.25	Proxy achieves a higher bit rate for Ethernet by 61,506.25 bits/s, indicating better speed.
9	Internet Protocol Version 4	99.98%	100.00%	0.02%	Proxy performs slightly better in terms of IPv4 efficiency.
10	Packets	82,319	98,720	16,401	Proxy handles 16,401 more IPv4 packets than VPN, showing better packet handling efficiency.
11	Bytes	16,46,380	19,74,400	3,28,020	Proxy transfers 3,28,020 more bytes for IPv4 than VPN, indicating better byte handling.
12	Bits/s	1,33,541.35	61,36,423.29	60,02,881.94	Proxy achieves a much higher bit rate for IPv4 by 60,02,881.94 bits/s, suggesting better speed.
13	User Datagram Protocol	99.82%	0.01%	-99.81%	VPN handles UDP traffic far better, with a 99.81% higher percentage than Proxy.
14	Packets	82,185	8	-82,177	VPN handles 82,177 more UDP packets than Proxy, indicating superior UDP handling efficiency.
15	Bytes	6,57,480	64	-6,57,416	VPN transfers 6,57,416 more bytes in UDP traffic, showing better efficiency.
16	Bits/s	4.33	-	4.33	VPN achieves a higher bit rate for UDP traffic (Proxy does not handle UDP traffic effectively).
17	Simple Service Discovery Protocol	0.01%	0.01%	0.00%	Both VPN and Proxy show identical performance in handling this protocol.
18	Packets	8	8	0	Both VPN and Proxy handle the same number of packets for this protocol.
19	Bytes	1,400	1,400	0	Both VPN and Proxy handle the same number of bytes for this protocol.
20	Bits/s	94.69	-	94.69	VPN achieves a higher bit rate for this protocol, with Proxy not handling it effectively.
21	Transmission Control Protocol	0.16%	99.99%	99.83%	Proxy handles TCP traffic much better, with a 99.83% higher percentage than VPN.
22	Packets	134	98,712	98,578	Proxy processes 98,578 more TCP packets than VPN, indicating better handling of TCP traffic.

23	Bytes	22,439	9,07,26,614	9,05,04,175	Proxy transfers 9,05,04,175 more bytes for TCP traffic, showing superior efficiency.
24	Bits/s	61,36,423.29	-	61,36,423.29	Proxy achieves a higher bit rate for TCP, showing better performance in managing TCP traffic.
25	Transport Layer Security	0.08%	11.32%	11.24%	Proxy handles TLS traffic significantly better, with an 11.24% higher percentage than VPN.
26	Packets	68	11,178	11,110	Proxy processes 11,110 more TLS packets than VPN, indicating better handling.
27	Bytes	19,759	9,01,88,574	8,81,28,815	Proxy transfers 8,81,28,815 more bytes for TLS traffic, showing much better efficiency.
28	Bits/s	61,00,032.19	-	61,00,032.19	Proxy achieves a much higher bit rate for TLS traffic, indicating superior performance.

In evaluating the performance of VPN and Proxy protocols across various metrics, both protocols achieve a frame efficiency of 100%, indicating equal performance in encapsulating and processing frames. However, Proxy handles 16,387 more packets than VPN, suggesting superior packet handling capabilities, while VPN transfers 81,09,347 more bytes, demonstrating better byte transfer efficiency. VPN also achieves a bit rate 1,61,00,000 bits/s higher than Proxy, reflecting superior speed in data transfer. For Ethernet traffic, both protocols perform equally well with 100% efficiency, but Proxy manages 16,387 more Ethernet packets and transfers 2,29,418 more bytes, achieving a bit rate 61,506.25 bits/s higher than VPN. In IPv4 management, Proxy shows a slight edge with 100% efficiency compared to VPN's 99.98%, handling 16,401 more packets and transferring 3,28,020 more bytes, with a bit rate 60,02,881.94 bits/s higher. For UDP traffic, VPN outperforms Proxy with 99.81% higher efficiency, handling 82,177 more packets and transferring 6,57,416 more bytes, achieving a higher bit rate as Proxy does not effectively handle UDP traffic. Both protocols perform equally in handling SSDP traffic (R. Li et al., 2024) with 0.01% efficiency, managing the same number of packets and bytes. In contrast, VPN achieves a higher bit rate for SSDP traffic. Proxy shows a remarkable 99.83% higher efficiency in TCP traffic, processing 98,578 more packets and transferring 9,05,04,175 more bytes, with a higher bit rate. Lastly, Proxy significantly outperforms VPN in TLS traffic (Badra & Hajjeh, 2006), (Zain ul Abideen et al., 2019), with an 11.24% higher efficiency, processing 11,110 more packets and transferring 8,81,28,815 more bytes, achieving a much higher bit rate, indicating superior performance in secure data transfer. the table 1 reveals that Proxy generally outperforms VPN in handling most types of traffic, including TCP, IPv4, and TLS, while VPN excels in managing UDP traffic. This analysis helps in selecting the appropriate protocol based on specific needs and performance requirements for different types of network traffic.

Comparative Analysis of Network Performance Metrics

A comparative analysis of network performance metrics involves evaluating and contrasting various performance indicators to understand how different network setups, such as VPNs (Virtual Private Networks) and proxy servers, perform under similar or varying conditions. This analysis helps in identifying strengths, weaknesses, and overall efficiencies in network operations, facilitating informed decision-making for optimization and troubleshooting.

Table 2. Provides a comparative analysis of network performance metrics between VPN and Proxy services.

Comparative Analysis of Network Performance Metrics				
SL NO	**Particulars**	**VPN**	**PROXY**	**Suggestion**
1	Packets	82333	98720	-16387

2	Bytes	102193905	94083690	8110215
3	Rel Start	110.37977	108.986745	1.393025
4	Duration	6.037431	6.054688	-0.017257

The VPN handled 82,333 packets, whereas the Proxy managed 98,720 packets. This results in a difference of -16,387 packets between the two services. The lower packet count in the VPN may indicate less frequent data transmission or potential packet loss compared to the Proxy. The VPN transmitted a total of 102,193,905 bytes, while the Proxy transmitted 94,083,690 bytes. This reflects an additional 8,110,215 bytes transferred via VPN. The higher byte count for the VPN suggests more substantial data throughput or potentially larger data payloads being processed. The VPN's relative start time was 110.37977 seconds, compared to the Proxy's 108.986745 seconds. This results in a slight delay of 1.393025 seconds for the VPN. The increased start time for the VPN could imply additional initialization or connection setup time relative to the Proxy. The total duration for VPN was 6.037431 seconds, while the Proxy's duration was 6.054688 seconds, showing a marginal difference of -0.017257 seconds. The negligible difference in duration suggests similar performance in terms of connection or data transfer time between the two services. The VPN exhibited a higher data transfer in bytes and slightly longer relative start time, which might be relevant when evaluating its performance compared to the Proxy. It could be beneficial to investigate further to understand the impact of these differences on overall network efficiency and user experience.

Packet Lengths Analysis for VPN and Proxy:

Packet Lengths Analysis is a crucial aspect of network traffic analysis that provides insights into the nature and distribution of data packets transmitted across a network. Understanding packet lengths helps in evaluating network performance, identifying potential issues, and optimizing data handling strategies.

Table 3. VPN Packet Lengths

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	82,333	1,241.23	42	1,467	0.9009	100%	4.04	36.16
0-19	0	-	-	-	0	0.00%	-	-
20-39	0	-	-	-	0	0.00%	-	-
40-79	80	51.9	42	54	0.0009	0.10%	0.03	59.494
80-159	900	141.09	93	159	0.0098	1.09%	0.44	63.357
160-319	9,494	186	160	317	0.1039	11.53%	0.73	63.365
320-639	288	489.14	320	637	0.0032	0.35%	0.12	62.658
640-1279	300	927.15	640	1,275	0.0033	0.36%	0.14	71.276
1280-2559	71,271	1,401.38	1,295	1,467	0.7798	86.56%	3.63	36.16
2560-5119	0	-	-	-	0	0.00%	-	-
5120 and greater	0	-	-	-	0	0.00%	-	-

Table 3 provides a comprehensive overview of packet lengths for VPN traffic, presenting data on packet counts, average lengths, minimum and maximum values, processing rates, and distribution percentages. The VPN manages a total of 82,333 packets with an average length of 1,241.23 bytes (Gao et al., 2020). The smallest packet recorded is 42 bytes, while the largest reaches 1,467 bytes. The rate of processing these packets is approximately 0.9009 milliseconds. The data shows a clear dominance of larger packets, particularly in the 1280-2559 bytes range, which constitutes 86.56% of the total packet count. This indicates that the majority of traffic consists of substantial data bursts, likely reflecting high-volume data transfers or large file transfers typical in VPN scenarios. The distribution of packet lengths across different ranges highlights a significant absence of packets in the smallest categories (0-19 bytes and 20-39 bytes), suggesting that very small packets are not a common feature of the VPN traffic. For packet lengths between 40-79 bytes and 80-159 bytes, the counts are relatively low, with 80 packets averaging 51.90 bytes and 900 packets averaging 141.09 bytes. This minimal representation

of smaller packets may imply that the VPN is optimized for handling larger, more substantial data transmissions. Packets in the 160-319 bytes range number 9,494 with an average length of 186.00 bytes, indicating a moderate proportion of medium-sized packets. The VPN also handles 288 packets in the 320-639 bytes range with an average length of 489.14 bytes, and 300 packets in the 640-1279 bytes range with an average length of 927.15 bytes. These figures suggest that while the VPN does process a variety of packet sizes, the majority of the data is concentrated in the larger packet size range. No packets are recorded in the 2560-5119 bytes or 5120 bytes and greater categories, reflecting that exceptionally large packets are either rare or non-existent in this VPN setup. The burst rates and start times for different ranges show that while there is significant activity in large packet ranges, the overall burst rate for the largest packet category (1280-2559 bytes) is 3.6300, indicating that large data bursts are processed efficiently without significant delay (Al-Fayoumi et al., 2022). In essence, the VPN's packet length data reveals a traffic pattern dominated by large packets, with a clear focus on high-volume data transfers. The absence of very small packets and the low burst rates for smaller sizes suggest an optimization towards handling substantial data efficiently, which is typical for VPN usage where large data streams are common.

Table 4: Proxy Packet Lengths

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	98,720	953.04	54	1,514	0.8346	100%	4.58	69.911
0-19	0	-	-	-	0	0.00%	-	-
20-39	0	-	-	-	0	0.00%	-	-
40-79	29,655	54.19	54	79	0.2507	30.04%	1.22	78.081
80-159	743	102.81	80	158	0.0063	0.75%	0.16	20.886
160-319	254	259.86	160	319	0.0021	0.26%	0.1	11.789
320-639	333	502.93	321	639	0.0028	0.34%	0.08	46.918
640-1279	18,917	1,119.96	640	1,277	0.1599	19.16%	1.02	78.081
1280-2559	48,818	1,454.00	1,289	1,514	0.4127	49.45%	2.92	69.912
2560-5119	0	-	-	-	0	0.00%	-	-
5120 and greater	0	-	-	-	0	0.00%	-	-

Table 4 details the packet lengths for Proxy traffic, offering insights into packet distribution, averages, and processing characteristics. The Proxy handles 98,720 packets with an average length of 953.04 bytes. The smallest packet is 54 bytes, and the largest is 1,514 bytes, with an average processing rate of 0.8346 milliseconds. The data shows a significant concentration of packets in the 1280-2559 bytes range, which makes up 49.45% of the total, indicating that a large portion of Proxy traffic involves substantial data transfers. This is somewhat similar to the VPN's traffic pattern but with a broader range of packet sizes (Kothapalli, 2023b). The Proxy’s data distribution includes notable counts of smaller packets, especially in the 40-79 bytes range, where 29,655 packets are recorded with an average length of 54.19 bytes. This suggests that the Proxy handles a higher volume of smaller packets compared to the VPN. Additionally, the 80-159 bytes range shows 743 packets with an average of 102.81 bytes, and the 160-319 bytes range includes 254 packets averaging 259.86 bytes (Guan et al., 2011). This indicates that the Proxy is also responsible for a variety of packet sizes, including a considerable number of medium-sized packets. Packets in the 320-639 bytes range amount to 333, with an average length of 502.93 bytes, while the 640-1279 bytes range includes 18,917 packets averaging 1,119.96 bytes. The Proxy shows a more diverse distribution compared to the VPN, with considerable activity in both smaller and larger packet categories. The absence of packets in the 2560-5119 bytes and 5120 bytes and greater categories suggests that extremely large packets are either rare or not present in the Proxy traffic. The burst rates and start times indicate that while there is a high concentration of larger packets, the processing rates for these packets are efficient. The Proxy’s packet length data indicates a varied traffic pattern with significant volumes of both small and large packets (Estan et al., 2003), [67]. This contrasts with the VPN, where traffic is predominantly larger packets. The Proxy's ability to handle a broad range of packet sizes efficiently points to its role in managing diverse traffic types, from small, frequent packets to larger data bursts.

I/O GRAPH:

The I/O graph data for VPN and Proxy networks provides a comprehensive comparison of network traffic patterns over a series of intervals. This data helps analyze how different types of network configurations influence packet transmission and overall traffic behavior.

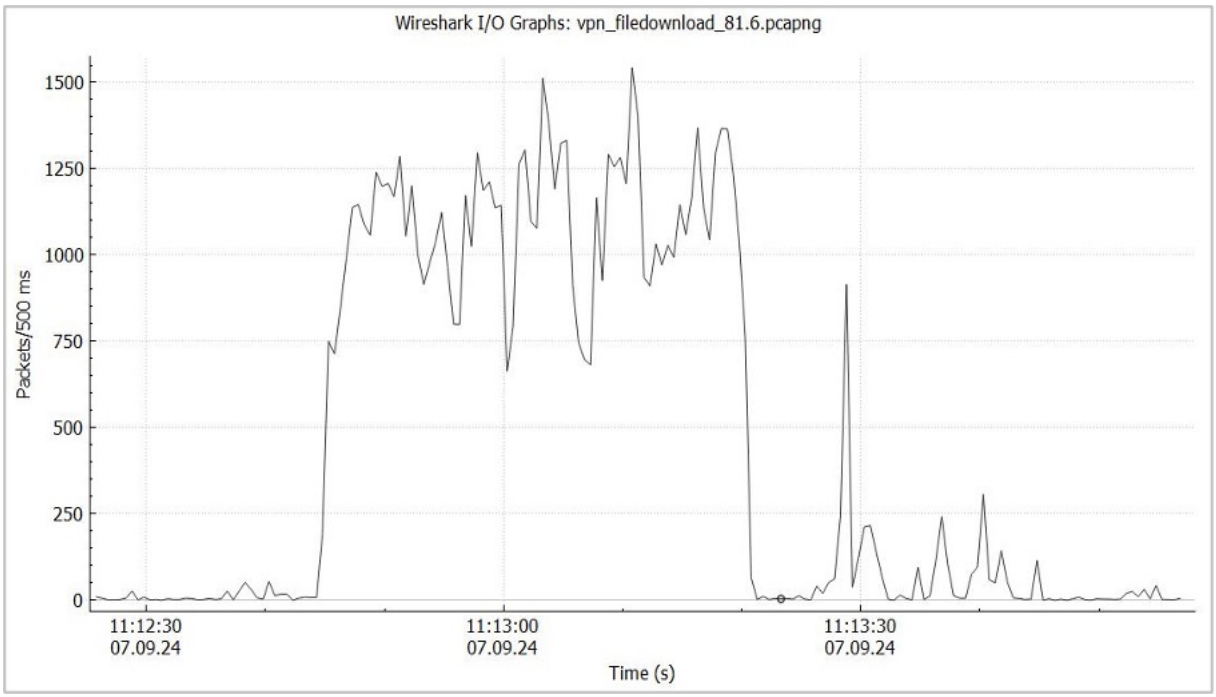


Figure 1 - VPN Traffic Analysis

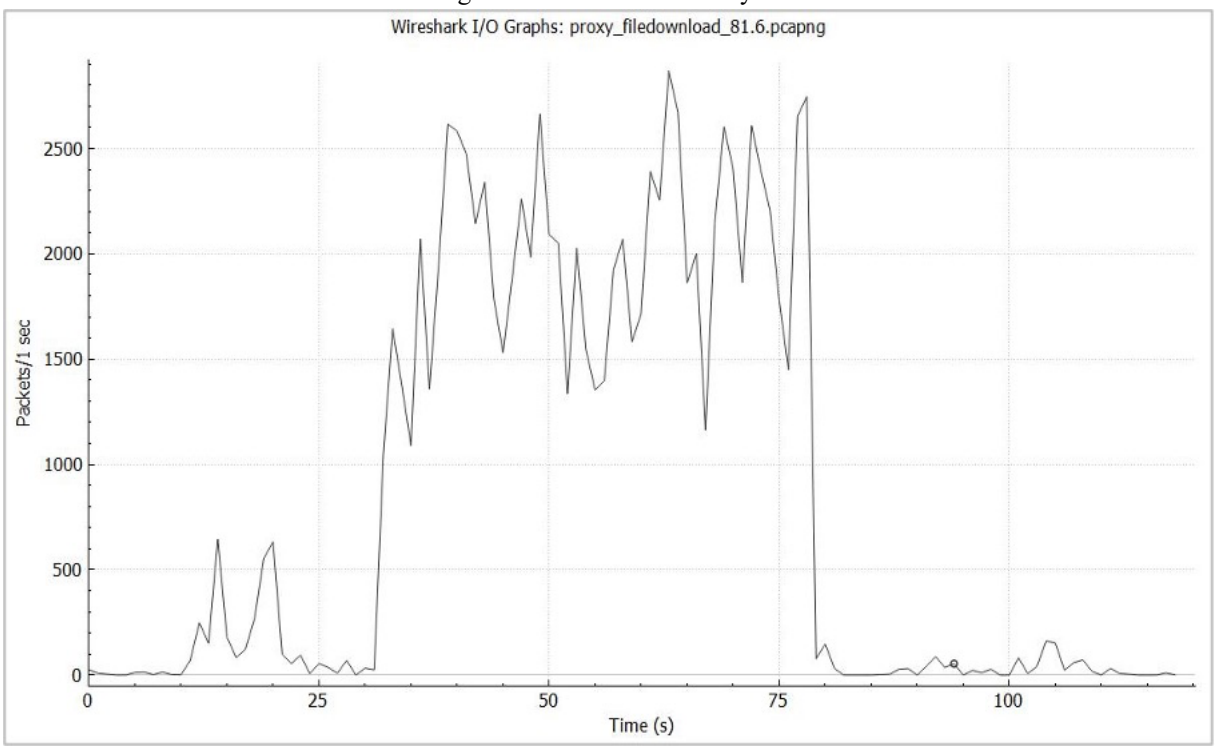
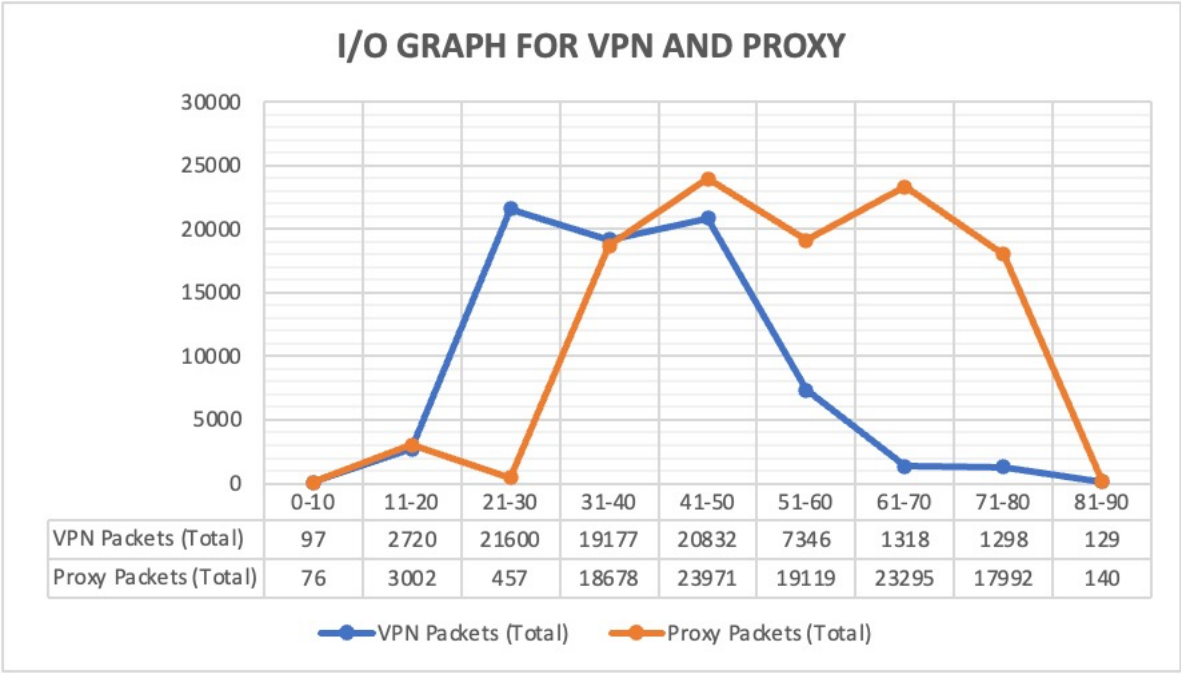


Figure 2 - Proxy Traffic Analysis

As illustrated in Figure 1, the VPN data reveals a pattern of relatively stable traffic with occasional significant peaks. In the initial intervals (0 to 10), the packet counts remain modest, ranging from 2 to 28 packets. This phase of stability is disrupted by a sharp increase at interval 19, where traffic surges dramatically to 946 packets. Such a spike suggests either a burst of data transmission or a high-volume operation during that moment. After this initial peak, VPN traffic continues

its upward trend, reaching a maximum of 2942 packets at interval 45, indicative of sustained intensive network activity or a period of high demand. However, this heightened traffic is followed by fluctuations between intervals 46 and 55, with packet counts varying from as high as 1845 to as low as 67 packets. These fluctuations likely correspond to alternating periods of intense and light network usage. A second major spike occurs at interval 63, where 953 packets are observed, followed by continued elevated traffic. Interestingly, the final intervals (80 to 91) exhibit a stark decline in packet counts, dropping as low as 2 packets. This sharp decrease likely signals a reduction in network activity or a significant drop in data transmission towards the end of the observed period, indicating the completion of the high-demand operations.

As illustrated in Figure 2, the Proxy traffic data exhibits a distinct pattern when compared to the VPN. The initial packet counts are higher, beginning at 24 packets in interval 0, followed by rapid fluctuations between 0 and 14 packets in the subsequent intervals. This volatility is punctuated by substantial bursts of activity, with notable peaks occurring at intervals 11, 12, and 14, where packet counts reach 69, 248, and 645 packets, respectively. These surges suggest periods of heavy data transfer or intensive use of the Proxy service. A significant burst is seen at interval 19, with packet counts rising to 554, marking a substantial increase in traffic. Following this, the Proxy data continues to exhibit variability, with several intervals showing elevated packet counts. Additional peaks are observed at intervals 33 and 39, with traffic surging to 1644 and 2615 packets, respectively. These periodic surges indicate specific events or periods of high demand, reflecting intensive use of the Proxy service. Towards the later part of the dataset, Proxy traffic reaches some of its highest levels, particularly between intervals 57 and 78, where packet counts range from 1924 to 2746. These high figures reflect extremely elevated network activity or significant data transmission during these intervals. However, towards the end, Proxy traffic drops sharply, with counts declining to 0 packets between intervals 82 and 85, signalling a significant reduction in network activity or a conclusion of high-demand operations.



	0-10	11-20	21-30	31-40	41-50	51-60	61-70	71-80	81-90
VPN Packets (Total)	97	2720	21600	19177	20832	7346	1318	1298	129
Proxy Packets (Total)	76	3002	457	18678	23971	19119	23295	17992	140

Figure 3 - Comparative Analysis of VPN and Proxy traffic across different time intervals

Figure 3 illustrates the comparative analysis of VPN and Proxy traffic across different time intervals, showcasing distinct variations in packet transmission patterns between the two network configurations. In the initial interval (0-10 seconds), the VPN network shows slightly higher activity with 97 packets compared to 76 for the Proxy. However, from intervals 11-20, the Proxy overtakes the VPN with 3002 packets against the VPN's 2720, reflecting a temporary surge in Proxy traffic. The VPN network sees a massive increase in the 21-30 second interval, transmitting 21,600 packets, while the Proxy drops significantly to just 457 packets. This suggests a high-demand period for VPN usage. Between 31-40 seconds, the Proxy network experiences a major recovery with 18,678 packets, closely trailing the VPN's 19,177, indicating similar usage levels. From 41-50 seconds, Proxy traffic surges past the VPN, reaching 23,971 packets compared to the VPN's 20,832, marking the Proxy's highest peak of activity. The trend reverses slightly in intervals 51-60, where VPN traffic drops to 7,346 packets, while the Proxy still maintains high levels with 19,119 packets. The 61-70 second interval sees a

dramatic drop in VPN traffic to 1,318 packets, while Proxy traffic rises to 23,295, the Proxy's second peak. In the final intervals, 71-80 and 81-90 seconds, Proxy traffic continues to outpace VPN, transmitting 17,992 and 140 packets compared to the VPN's 1,298 and 129 packets, respectively. These observations highlight that while the VPN experiences periods of intense activity, Proxy traffic shows more consistent bursts of high traffic over the observed intervals. In finish, the I/O graph data provides a clear comparative analysis of VPN and Proxy network traffic patterns. VPN traffic demonstrates periods of stability interspersed with significant peaks, reflecting high-demand periods or intensive data transfers. This results in fluctuating network activity with notable surges and declines. Conversely, Proxy traffic exhibits more consistent bursts of high activity, with multiple peaks indicating periods of intensive use or high demand. The data reveals that while VPNs experience pronounced spikes followed by drops, proxies show sustained high activity over time. This comparative insight underscores the distinct traffic behaviors of each network configuration, guiding their application based on specific needs for stability, peak demand, and overall network performance.

Comparative Overview of VPN and Proxy Protocols for Library Systems

VPNs and proxies offer distinct advantages for library systems, catering to different needs. VPNs ensure secure, encrypted access to sensitive library data and internal systems, making them ideal for protecting confidential information and enabling remote administrative tasks. Proxies enhance user privacy by masking IP addresses, improve access to restricted content, and optimize performance through caching. Libraries may use VPNs for secure connections and proxies to manage web access and privacy, depending on their specific requirements.

Table 5. Comparison of VPN and Proxy Protocols for Library Systems

Aspect	VPN (Virtual Private Network)	Proxy Server
Definition	A VPN creates a secure and encrypted connection over a public network, effectively extending a private network across the internet.	A Proxy server acts as an intermediary between a client and the destination server, relaying requests and responses.
Purpose	To provide secure, encrypted access to a private network from a remote location, ensuring confidentiality and integrity of data.	To facilitate access to resources, enhance privacy, or bypass geographic restrictions by acting as a gateway between the client and the server.
Architecture	**Client**: Software or device that establishes a connection to the VPN server.	**Client**: Application or browser making requests to the proxy.
	VPN Server: Hosts the VPN service and manages encrypted connections.	**Proxy Server**: Receives client requests, processes them, and forwards them to the destination server.
	Tunnel: Encrypted pathway through which data is transmitted.	**Destination Server**: The server hosting the content requested by the client.
	Gateway: Interfaces with the internet and internal network.	
Encryption	Uses advanced encryption standards (e.g., AES) to secure data in transit, protecting it from eavesdropping and tampering.	Encryption is limited to protocols such as HTTPS; otherwise, data is typically transmitted in plaintext.
Authentication	Supports various authentication methods, including usernames/passwords, certificates, and multi-factor authentication to ensure secure access.	Authentication methods vary; can include basic authentication, OAuth, or none, depending on the configuration.
Performance Impact	May introduce some latency due to the overhead of encryption and secure tunneling, but generally maintains good performance for data-sensitive applications.	Typically has minimal impact on performance as it does not encrypt data; primarily focuses on request handling and routing.

Suitability for Libraries	Securing remote access to the library's internal systems. Protecting sensitive data, such as patron information and library transactions. Ensuring secure access for remote staff and users. Enabling secure connections to remote databases and digital resources. Enhances security and confidentiality. Supports secure remote work and access to internal systems.	Enhancing privacy for users accessing library resources. Bypassing regional restrictions on digital content. Improving access speed through caching of frequently requested content. Simplifies access to web resources. Facilitates content access control and monitoring. Can help manage web traffic and reduce load on library servers.

Table 5 illustrated the distinctions between VPN and Proxy protocols and their applicability to library systems. VPNs are crucial for libraries that prioritize secure access to sensitive information. For example, libraries often handle patron records, internal databases, and proprietary information that must be kept confidential. VPNs provide a secure tunnel through which data is transmitted, ensuring that information sent over the internet is encrypted and protected from unauthorized access. This is particularly important for library staff who need to perform administrative tasks or manage resources remotely. By using a VPN, library staff can securely connect to the library's internal systems from various locations, whether they are working from home, traveling, or accessing the system from a branch office. The confidentiality provided by VPNs helps in safeguarding library data and communications, adding an extra layer of protection against potential cyber threats such as data breaches or unauthorized intrusions. Proxies, on the other hand, offer a different set of benefits that are valuable to libraries. They enhance user privacy by masking the IP addresses of library patrons and anonymizing their web traffic. This is particularly useful when patrons access online resources, as it helps in maintaining their privacy and reducing tracking by external entities. Additionally, proxies can be used to bypass geographic restrictions on digital content, enabling users to access resources that might be limited based on their location. For instance, some digital databases or e-books may only be available in certain countries. A proxy can help circumvent these restrictions, allowing users to access a broader range of resources. Moreover, proxies can improve the performance of web-based resources by caching frequently accessed content. This reduces the load on library servers and speeds up access to resources, providing a more efficient user experience. VPNs and proxies serve complementary roles in a library environment. VPNs are ideal for ensuring secure, remote access to sensitive data and protecting library communications. Proxies are beneficial for enhancing user privacy, bypassing content restrictions, and improving access speed through caching. Libraries should choose the solution that best aligns with their security, privacy, and performance needs, or consider using both technologies to cover a broader range of requirements.

Results and Discussion

The comparative analysis of VPN and Proxy protocols highlights key distinctions in packet lengths and traffic patterns, providing a comprehensive understanding of how each technology manages network data. This evaluation is crucial for institutions such as libraries, where network performance, security, and privacy are of paramount importance.

- **VPN Traffic Characteristics**

VPN traffic predominantly comprises larger packets, especially in the 1280-2559 bytes range, which constitutes 86.56% of the total packet count. This dominant packet size suggests that VPNs are highly efficient in handling large data transmissions, particularly those typical of high-volume or bulk file transfers, such as database synchronization or remote backups of library resources. The average packet length of 1,241.23 bytes, with a range from 42 bytes to 1,467 bytes, underscores the VPN's capacity to maintain stable and substantial data throughput. One of the most significant observations is the absence of very small packets and the minimal occurrence of smaller-sized packets, which indicates that VPNs are optimized for large-scale data exchanges. This characteristic is particularly advantageous for libraries that frequently transfer large datasets, such as digital archives, academic journals, or media content, across secure networks. The processing rate of 0.9009 milliseconds further highlights VPNs' efficiency in maintaining continuous and secure data streams, ensuring minimal interruptions or delays in data transmission. Additionally, VPN traffic patterns reveal periods of stability interspersed with significant peaks, which likely reflect high-demand operations. These peaks may correspond to large-scale library operations such as system-wide backups, resource sharing between branches, or high-traffic user access periods when numerous users are accessing digital resources simultaneously. Peaks observed at intervals 19 and 45, where traffic surges dramatically, emphasize the VPN's ability to manage sudden bursts of activity without compromising security or performance. This capability is invaluable for libraries that require uninterrupted, secure remote access to

sensitive information, particularly for administrative tasks or remote users.

Proxy Traffic Characteristics

In contrast, Proxy traffic exhibits a more diverse range of packet sizes, with an average packet length of 953.04 bytes and a range from 54 bytes to 1,514 bytes. Unlike VPNs, which are optimized for larger, consistent data streams, proxies manage a broader spectrum of packet sizes, accommodating both small and large data requests. This flexibility is advantageous in environments where diverse traffic types need to be managed efficiently. A notable characteristic of Proxy traffic is the significant concentration of packets in the 1280-2559 bytes range (49.45%), similar to VPN traffic, which suggests that proxies are also capable of handling substantial data transfers. However, the presence of smaller packets, particularly those in the 40-79 bytes range, indicates that proxies are equally adept at managing lightweight data requests, such as simple webpage requests or metadata retrieval. This ability to handle diverse traffic efficiently positions proxies as highly flexible tools, particularly useful for caching frequently accessed content and enhancing the speed of web-based services.

The processing rate for Proxy traffic, approximately 0.8346 milliseconds, demonstrates the technology's efficiency in handling bursts of traffic across various sizes. The periodic bursts of activity, observed at intervals 11, 12, and 14, illustrate the Proxy's responsiveness to sudden increases in network demand, making it well-suited for managing user-generated traffic, such as patrons accessing e-books, databases, or online catalogs. The consistent bursts of high activity in later intervals further reinforce the Proxy's capacity to manage fluctuating traffic loads while maintaining efficient performance.

Comparative Insights

When comparing VPN and Proxy protocols, key differences emerge in their approach to managing network traffic. VPN traffic is characterized by a predominance of large packets, with minimal representation of smaller packets. This suggests that VPNs are specifically optimized for managing large data streams, making them ideal for securing bulk data transfers that require encryption and privacy. In contrast, Proxy traffic shows a more varied packet size distribution, handling both small and large packets, indicating that proxies are designed to manage diverse traffic types. This makes them more suitable for scenarios where flexibility in traffic management is critical, such as optimizing access to web-based resources or bypassing regional content restrictions. The I/O graph analysis adds further nuance to this comparison. VPN traffic patterns display relatively stable activity with occasional significant peaks, particularly during periods of high demand or intensive data transfers. These spikes indicate the VPN's ability to handle substantial, concentrated bursts of data, such as when multiple users simultaneously access the library's digital resources. Conversely, Proxy traffic exhibits higher initial packet counts and significant variability across intervals. This variability, punctuated by frequent bursts of activity, highlights the Proxy's role in managing more dynamic traffic loads, making it ideal for handling multiple concurrent user requests while maintaining network efficiency.

Implications for Library Network Management

Both VPNs and proxies serve complementary roles in library network management, offering distinct advantages based on the institution's specific needs. VPNs provide secure, encrypted connections that are essential for remote access to sensitive information, making them invaluable for library staff conducting administrative tasks or for users accessing restricted databases remotely. VPNs excel in protecting data integrity and ensuring that sensitive communications remain secure, even in high-traffic situations. However, their encryption and data handling mechanisms may introduce latency, making them less suited for scenarios that prioritize speed over security.

Proxies, on the other hand, offer greater flexibility and efficiency in managing web traffic. By caching frequently accessed content and improving load times, proxies enhance the user experience for patrons accessing digital resources. Additionally, proxies enable libraries to monitor and control internet usage, implementing content filtering or bypassing regional restrictions to provide users with broader access to global information. Proxies generally have minimal performance impact, making them ideal for environments where speed is crucial, but the data being transmitted does not require the stringent security provided by VPNs.

Recommendations for Libraries

Libraries should carefully consider their specific needs when deciding between VPNs, proxies, or a combination of both technologies. For institutions prioritizing security, such as protecting patron data or safeguarding access to proprietary digital resources, VPNs are the ideal solution. Their ability to secure large data transfers and ensure encrypted communication makes them indispensable for libraries handling sensitive data. On the other hand, for institutions focused

on enhancing user access and performance, proxies offer significant advantages. Their ability to manage diverse traffic types, improve load times, and facilitate access to restricted content makes them particularly useful for public-facing services. Libraries that provide extensive online resources to patrons can benefit from the caching capabilities of proxies, which reduce server load and enhance the overall user experience. Ultimately, libraries may find that a hybrid approach using VPNs for secure, administrative tasks and proxies for public access services provides the best balance between security, performance, and flexibility. By leveraging the strengths of both technologies, libraries can create a network infrastructure that not only protects their resources but also ensures efficient, user-friendly access to digital services.

Conclusion

Based on the analysis and findings, as well as insights from the literature review, it is clear that both VPNs and Proxy protocols play significant, yet distinct, roles in library network management. Throughout the literature, as emphasized by Bhatti et al. (2024), VPNs are recommended for their robust security, emphasizing that the best choice depends on the specific needs of the institution. VPNs are universally praised by scholars (Huang & Frahim, 2008; Kose et al., 2024) for their robust security features. These studies consistently recommend VPNs for environments where data security is paramount, such as libraries handling sensitive information like patron records or proprietary digital resources. VPNs excel in providing encrypted, secure access to internal systems and remote resources, making them indispensable for protecting sensitive data. The methodology in this study confirmed that VPNs handle large packet sizes efficiently, especially in high-volume data transfers, which is crucial for secure administrative tasks and resource sharing across library systems.Conversely, Proxy servers are often cited (Pavlicek & Sudzina, 2018; Bhatti et al., 2024) for their flexibility and performance in managing diverse traffic types. As demonstrated through the analysis, Proxies handle a broader range of packet sizes and provide better optimization for web traffic. This makes them an ideal choice for libraries looking to enhance user experience by improving load times and enabling access to geographically restricted e-resources. The methodology's findings support the literature by showing Proxies' ability to manage smaller packet sizes efficiently and maintain high performance in environments with varying traffic demands.

From a methodological standpoint, this study simulated typical file transfers, providing a real-world evaluation of both protocols. VPNs excelled in managing large data bursts securely, while Proxies were more effective at optimizing overall web traffic, particularly for resource-heavy environments with remote access needs. The findings align with the consensus in the literature that each protocol has its best use case: VPNs for securing sensitive data and Proxies for enhancing accessibility and speed. In conclusion, as both the literature and this study suggest, VPNs are the recommended solution for libraries prioritizing data security, encryption, and protection of internal systems. Conversely, Proxies are best suited for enhancing user access to e-resources and optimizing general web traffic. For libraries with both security and performance needs, a hybrid approach leveraging both VPNs and Proxies will offer the most effective solution. By understanding when and how to use each technology, libraries can develop a well-rounded, secure, and efficient network infrastructure that meets the evolving demands of digital resource management and access.

Reference

1. Abrams, M., Standridge, C. R., Abdulla, G., Williams, S., & Fox, E. A. (1995). Caching proxies: Limitations and potentials. 119–133. https://doi.org/10.1145/3592626.3592635
2. Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. (2024). Virtual private networks (VPN): A conceptual review of security protocols and their application in modern networks. Engineering Science & Technology Journal, 5(4), 1452–1472. https://doi.org/10.51594/estj.v5i4.1076
3. Al-Fayoumi, M., Al-Fawa'reh, M., & Nashwan, S. (2022). VPN and Non-VPN Network Traffic Classification Using Time-Related Features. Computers, Materials & Continua, 72(2). https://doi.org/10.32604/cmc.2022.025103
4. Azwee, K., Alkhattali, M., & Dow, M. (2023). Exploring the Effectiveness of VPN Architecture in Enhancing Network Security for Mobile Networks: An Investigation Study. International Journal of Network Security & Its Applications (IJNSA), 15. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4598386
5. Badra, M., & Hajjeh, I. (2006). Enabling VPN and secure remote access using TLS protocol. 308–314. https://doi.org/10.1109/WIMOB.2006.1696366
6. Balachandran, S., & Dominic, J. (2023). Pioneering a Prototype VPN-Based Cloud Strategy for Streamlined Library Management. Library Philosophy & Practice. https://digitalcommons.unl.edu/libphilprac/7949/
7. Bhatti, D. S., Sidrat, S., Saleem, S., Malik, A. W., Suh, B., Kim, K.-I., & Lee, K.-C. (2024). Performance analysis:

Securing SIP on multi-threaded/multi-core proxy server using public keys on Diffie–Hellman (DH) in single and multi-server queuing scenarios. Plos One, 19(1), e0293626. https://doi.org/10.1371/journal.pone.0293626

8. Bringhenti, D., Sisto, R., & Valenza, F. (2024). Automating VPN configuration in computer networks. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2024.3409073

9. Burnside, M., Clarke, D., Mills, T., Maywah, A., Devadas, S., & Rivest, R. (2002). Proxy-based security protocols in networked mobile devices. 265–272. https://doi.org/10.1145/508791.508845

10. Cha, S.-C., Hsu, T.-Y., Xiang, Y., & Yeh, K.-H. (2018). Privacy enhancing technologies in the Internet of Things: Perspectives and challenges. IEEE Internet of Things Journal, 6(2), 2159–2187. https://doi.org/10.1109/JIOT.2018.2878658

11. Chapman, C. (2016). Network performance and security: Testing and analyzing using open source and low-cost tools. Syngress. Google_Book_link

12. Cleary, J. (1994). Academic libraries, networking and technology: Some recent developments. The Australian Library Journal, 43(4), 235–256. https://doi.org/10.1080/00049670.1994.10755695

13. Covey, D. T. (2003). The need to improve remote. Portal: Libraries and the Academy, 77, 599.

14. Dikshit, P., Sengupta, J., & Bajpai, V. (2023). Recent trends on privacy-preserving technologies under standardization at the IETF. ACM SIGCOMM Computer Communication Review, 53(2), 22–30. weblink

15. Estan, C., Savage, S., & Varghese, G. (2003). Automatically inferring patterns of resource consumption in network traffic. 137–148. https://doi.org/10.1145/863955.863972

16. Gao, P., Li, G., Shi, Y., & Wang, Y. (2020). VPN traffic classification based on payload length sequence. 241–247. https://doi.org/10.1109/NaNA51271.2020.00048

17. Guan, J., Zhou, H., Yan, Z., Qin, Y., & Zhang, H. (2011). Implementation and analysis of proxy MIPv6. Wireless Communications and Mobile Computing, 11(4), 477–490. https://doi.org/10.1002/wcm.842

18. Harmening, J. (2025). Virtual private networks. In Computer and Information Security Handbook (pp. 979–992). Elsevier. https://booksite.elsevier.com/samplechapters/9780123704719/Sample_Chapters/01~Front_Matter.pdf

19. Huang, Q., & Frahim, J. (2008). SSL Remote Access VPNs (Network Security). Cisco Press.

20. Janbeglou, M., & Brownlee, N. (2016). Identifying tunneled proxies through passively monitoring network traffic. 63–69. Google_book_Link

21. Kim, H.-C., Lee, D., Chon, K., Jang, B., Kwon, T., & Choi, Y. (2010). Performance impact of large file transfer on web proxy caching: A case study in a high bandwidth campus network environment. Journal of Communications and Networks, 12(1), 52–66. https://doi.org/10.1109/JCN.2010.6388434

22. Kose, B. O., Coskun, V., Coskun, A., & Yaya, S. (2024). An innovative approach to virtual private networks for enhancing digital security and accessibility. 1–5. https://doi.org/10.1109/HORA61326.2024.10550795

23. Kothapalli, S. C. (2023). Measurement, analysis, and system implementation of internet proxy servers. https://www.proquest.com/openview/39c164d5c9b5728fbbc7bff02fb276f6/1?pq-origsite=gscholar&cbl=18750&diss=y

24. Kovacs, A. (2024). Comparative analysis of traditional and modern proxy solutions in cyber security. International Journal of Communication Networks and Information Security (IJCNIS), 16(2), 19–32. https://www.ijcnis.org/index.php/ijcnis/article/view/6689

25. Kurniadi, D. D. (2015). The difference between using proxy server and VPN. Jurnal Sisforma, 2(1), 19–22. http://repository.unika.ac.id/id/eprint/6909

26. Lacković, D., & Tomić, M. (2017). Performance analysis of virtualized VPN endpoints. 466–471. https://doi.org/10.23919/MIPRO.2017.7973470

27. Lawas, J. B. R., Vivero, A. C., & Sharma, A. (2016). Network performance evaluation of VPN protocols (SSTP and IKEv2). 1–5. https://doi.org/10.1109/WOCN.2016.7759880

28. Li, B., Golin, M. J., Italiano, G. F., Deng, X., & Sohraby, K. (1999). On the optimal placement of web proxies in the internet. 3, 1282–1290. https://doi.org/10.1109/INFCOM.1999.752146

29. Li, R., & Cao, X. (2024). Research on the design of network security system for natural resources big data platform based on zero-trust architecture. 13228, 360–366. https://doi.org/10.1117/12.3038292

30. Li, R., Li, Q., Lin, T., Zou, Q., Zhao, D., Huang, Y., Tyson, G., Xie, G., & Jiang, Y. (2024). DeviceRadar: Online IoT device fingerprinting in ISPs using programmable switches. IEEE/ACM Transactions on Networking. https://doi.org/10.1109/TNET.2024.3398778

31. Liebl, G., Tu, W., & Steinbach, E. (2007). Proxy-based transmission strategies for wireless video streaming. 201–210. https://doi.org/10.1109/PACKET.2007.4397042

32. Mahmmod, K. F., Azeez, M. M., & Ahmed, M. A. (2020). IPsec cryptography for data packets security within VPN tunneling networks communications. 1–8. https://doi.org/10.1109/ICELTICs50595.2020.9315407
33. Mani, A., Vaidya, T., Dworken, D., & Sherr, M. (2018). An extensive evaluation of the internet's open proxies. 252–265. https://doi.org/10.1145/3274694.3274711
34. Miracle, N. O. (2024). The importance of network security in protecting sensitive data and information. International Journal of Research and Innovation in Applied Science, 9(6), 259–270. https://doi.org/10.51584/IJRIAS.2024.906024
35. Morsli, N., Boulhilate, T., Ibourk, M., Hilali, S., Carlier, F., & Bahnasse, A. (2024). Performance assessment of the impact of the encryption layer on a highly available campus network. Procedia Computer Science, 238, 572–577. https://doi.org/10.1016/j.procs.2024.06.062
36. Naidu, D. R., & Jha, M. D. (2023). Detection technique to trace IP behind VPN/Proxy using machine learning. International Journal of Next-Generation Computing, 14(1). https://doi.org/10.47164/ijngc.v14i1.1006
37. Neto, E. P. de A. R. J. (2023). Paying for privacy in a digital age: Willingness to pay for attributes in a VPN (Virtual Private Network) service, and its relation to privacy literacy. https://repositorio.iscte-iul.pt/handle/10071/28497
38. Newman, R. C. (2009). Computer Security: Protecting Digital Resources. Jones & Bartlett Publishers. Google_Book_link
39. Pavlicek, A., & Sudzina, F. (2018). Use of virtual private networks (VPN) and proxy servers: Impact of personality and demographics. 108–111. https://doi.org/10.1109/ICDIM.2018.8846991
40. Quick, D., & Choo, K.-K. R. (2014). Google Drive: Forensic analysis of data remnants. Journal of Network and Computer Applications, 40, 179–193. https://doi.org/10.1016/j.jnca.2013.09.016
41. Radchenko, V., Alekseenko, A., Rusnak, A., & Fomin, S. (2024). Overcoming challenges in deep inspect of VPN and proxy by deep learning. 2701(1), 012106. https://doi.org/10.1088/1742-6596/2701/1/012106