ANALYSIS OF THE EFFECTIVENESS OF SQUID PROXY IN WEBSITE FILTERING IN A NETWORK ENVIRONMENT

Idris Putra Hatoguan [1], Cristian Josua [2], Ahmad Denil [3], Bob Valentino [4], Pedro Stella Mario Meyar [5], Arnita [6]
[1,2,3,4,5,6] Computer Science, Universitas Negeri Medan
Jalan Willem Iskandar, Pasar V Medan Estate, Percut Sei Tuan, Deli Serdang, Sumatera Utara, Indonesia
Idrisputra76@gmail.com

ABSTRAK

The increasing dependence on internet technology in daily activities has brought both benefits and challenges, particularly regarding productivity and network security. Unrestricted access to all types of websites may lead to decreased efficiency, bandwidth waste, and exposure to harmful or inappropriate content. Therefore, website filtering mechanisms are necessary to maintain a healthy and secure network environment. This study aims to analyze the effectiveness of implementing Squid Proxy as a website filtering solution within a local network environment. Which includes stages such as problem identification, data collection, system design, product testing, and evaluation. The proxy system was configured using Squid Proxy with Access Control Lists (ACLs) on an Ubuntu 22.04 server to regulate user access, restrict specific domains, and monitor traffic activities. Testing was carried out using Wireshark to measure changes in bandwidth performance and access control effectiveness. The results demonstrate that Squid Proxy can efficiently block access to unwanted websites, enhance browsing speed through caching, and improve bandwidth utilization. Additionally, the integration of ACL-based filtering with user authentication ensures better access management and reduces security risks such as malware infiltration and data misuse. Overall, the findings confirm that Squid Proxy is a reliable and cost-effective open-source firewall solution that enhances network performance, increases bandwidth efficiency, and provides a secure digital environment for users.

Kata kunci : *Squid Proxy, website filtering, Access Control List (ACL), network security, bandwidth management, open-source firewall.*

1. INTRODUCTION

The rapid development of information technology has had both positive and negative impacts on human life. The internet, as the primary means of global information exchange, allows users to access a wide variety of content quickly and easily. However, despite its benefits, the internet also opens up opportunities for unproductive access and disrupts network efficiency. This phenomenon is increasingly worrying because it not only impacts learning effectiveness but also impacts work productivity and computer network security.

Website filtering efforts have been widely implemented using proxy server software. One frequently used tool is Squid Proxy. Sitorus et al. [1] demonstrated that Squid Proxy is capable of filtering websites without any site limitations, making it relevant for building a healthier and more efficient network environment. To increase filtering effectiveness, some researchers have combined Squid with artificial intelligence methods. For example, Ramaditia et al. [2] used a Naïve Bayes Classifier combined with the JADE automated agent. The results demonstrated a high level of accuracy in website classification, and the system automatically updated Access Control List (ACL) rules.Selain itu, Husaini dkk. [3] membandingkan performa Squid Proxy dengan metode Layer 7 Protocol. Hasil uji performa menunjukkan bahwa Squid Proxy lebih cepat (0,518 detik) sekaligus lebih efektif dalam melakukan penyaringan. Kurniawan dkk. [4] juga menegaskan bahwa implementasi Squid Proxy pada Mikrotik tidak hanya mampu menyaring website pada jadwal tertentu, tetapi juga meningkatkan efisiensi penggunaan bandwidth. Penelitian serupa dilakukan oleh Rosihan & Apriyadi [5] yang menekankan bahwa ACL dalam Squid sangat efektif untuk membatasi akses, dan fitur caching mempercepat waktu akses.

In a modern context, Squid Proxy has also proven relevant for the latest Linux-based systems. Artika et al. [6] implemented Squid Proxy on Ubuntu 22.04 and found a 20% increase in network performance and was effective for filtering unproductive content. Gea et al. [7] demonstrated that Squid Proxy with ACLs can minimize bandwidth leakage while controlling access granularly, thus supporting network security.

Another study conducted by Dwiyatno et al. [8] implemented Squid Proxy on a community ISP. The results showed that Squid functioned as both a website filter and network security, especially for low-cost internet service providers. Meanwhile, Lin & Yao [9] introduced a double decision tree algorithm for firewall anomaly detection, which was proven to save 33% on detection time and is relevant as a complement to Squid-based filtering. Meanwhile, Prasetyo [10] demonstrated that Squid Proxy, combined with the Address List and Delay

Pools methods, can perform dual functions: filtering websites while managing bandwidth usage fairly.

Thus, it can be concluded that Squid Proxy is a technological solution capable of not only filtering websites but also supporting bandwidth efficiency and network security. Previous studies have shown that combining Squid with modern methods such as machine learning, ACLs, and firewall algorithms further enhances its effectiveness. Therefore, this research is crucial to analyze Squid Proxy's role in creating a healthy, secure, and efficient digital environment.

2. LITERATURE REVIEW

2.1. Theroetical Review

a. Squid Proxy Server
   Squid is an open-source proxy application that functions as a caching proxy and web content filter. Squid allows network administrators to control internet traffic, speed up access through caching, and filter websites using Access Control Lists (ACLs).
b. Access Control List (ACL)
   ACLs in Squid are rules used to determine which websites or services can be accessed by network users. ACLs enable filtering based on IP addresses, domains, or specific URL patterns.
c. Website Filtering
   Filtering is a technique for restricting access to websites deemed inappropriate or unproductive. Filtering can be based on blacklists, machine learning, or integration with firewalls.
d. Bandwidth Management
   One of Squid's additional functions is the ability to manage bandwidth usage. With features like Delay Pools and Address Lists, administrators can allocate bandwidth fairly while preventing excessive access to irrelevant websites.
e. Network Security
   Using Squid Proxy supports network security by preventing unauthorized access, reducing bandwidth leaks, and improving control over internet traffic. When combined with firewall anomaly detection methods or artificial intelligence algorithms, its functionality can be even more optimal.

2.2. Related Work

Several previous studies have examined the effectiveness of Squid Proxy and its application in website filtering. Research by Sitorus et al. (2024) demonstrated that Squid Proxy combined with Mikrotik can effectively filter websites in a network environment.

Approach integrating Squid Proxy with the Naïve Bayes Classifier and JADE. The results of this study demonstrated that the combination of artificial intelligence-based filtering methods can significantly improve system accuracy. Furthermore, A comparison between the Layer 7 Protocol method and Squid Proxy in website filtering showed that Squid Proxy was superior in stability and efficiency compared to the Layer 7 Protocol, especially in networks with a large number of users [1]. Another study emphasized the role of Squid Proxy in network traffic monitoring, highlighting that Squid is not only useful for filtering but also helps network administrators optimize bandwidth management [2]. Furthermore, the implementation of Squid Proxy in conjunction with Zabbix within the Healthy Internet program demonstrated improved control over internet traffic and enhanced network security [3].

2.3. Research Model and Prosedur

a. Research Location and Time
   The research was conducted at one of the study members' boarding houses, which had a Wi-Fi network, from September to October 2025. The research stages included system design, Squid Proxy configuration, testing, and evaluation.
b. Types of research
   This research uses the Research and Development (R&D) method as described in [4]. R&D is a research method used to develop a specific product and test its effectiveness. In this study, the product developed is a website filtering system based on Squid Proxy with ACL.
c. Research design
   The research design used was the R&D development model as described in [4], with the following stages:
   - Potential and Problem Identification: identifying obstacles to using a network without a filtering system.
   - Data Collection: searching for references on Squid and ACL configurations.
   - Product Design: creating a proxy system configuration and network topology diagram.
   - Design Revision: refining the system design based on validation results.
   - Product Trial: implementing the system on a laptop network.
   - Product Revision: improvements after initial trials.
   - Limited Usage Testing: user testing and feedback gathering.
d. Data Collection Techniques
   The data collection techniques used in this study included:
   - Observation: observing network traffic activity before and after implementing Squid Proxy.
   - Documentation: recording Squid server configurations and logs.
   - Technical Measurement: conducting bandwidth and website access tests using software such as Wireshark

e. Research Instruments
The research instruments used consisted of:
- Hardware: computer server, router, and client PC.
- Software: Ubuntu 22.04, Squid Proxy Server, and Wireshark.

f. Research Procedures
The research procedures are structured narratively as follows:
- Preparation: Install the Ubuntu operating system and Squid Proxy Server on the laboratory server.
- Design: Configure the squid.conf file and create an Access Control List (ACL) based on the restricted domains.
- Implementation: Connect clients to the proxy network and test website access.
- Observation: Record log results and user responses to website access.
- Evaluation: Analyze bandwidth test data and blocker effectiveness.
- Product Revision: Adjust configurations to optimize system performance.

3. RESEARCH METHODS

3.1. Research Location and Time

This research was conducted in one of the study participants' dormitories with a Wi-Fi network, from September to October 2025. The research stages included system design, Squid Proxy configuration, testing, and evaluation.

3.2. Research Type

This research is a research and development (R&D) study, as proposed by Sugiyono (2019). This method is used to develop a specific product and test its effectiveness. The product developed in this study is a website filtering system based on the Squid Proxy Server with an Access Control List (ACL) feature implemented on the Ubuntu 22.04 operating system.

3.3. Research Design

The research design used is Sugiyono's (2019) R&D development model with the following stages:

a. Potential and Problem Identification: identifying obstacles to network use without a filtering system.
b. Data Collection: searching for references on Squid and ACL configurations.
c. Product Design: creating proxy system configurations and network topology diagrams.
d. Product Trial: System implementation on a laptop network.
e. Product Revision: Improvements after initial trials.
f. Limited Usage Test: User testing and feedback collection.

3.4. Research Instruments

The research instruments used consisted of:

a. Hardware: computer server, router, and client PC.
b. Software: Ubuntu 22.04, Squid Proxy Server, and Wireshark.

3.5. Research Procedures

The research procedures are structured narratively as follows:

a. Preparation: Installation of the Ubuntu operating system and Squid Proxy Server on a laboratory server.
b. Design: Configuration of the squid.conf file and creation of an Access Control List (ACL) based on restricted domains.
c. Implementation: Connecting clients to the proxy network and testing website access.
d. Observation: Recording log results and user responses to website access.
e. Evaluation: Analyzing bandwidth test data and blocking effectiveness.
f. Product Revision: adjust configuration to optimize system performance.

Figure 1. Research Method Flowchart

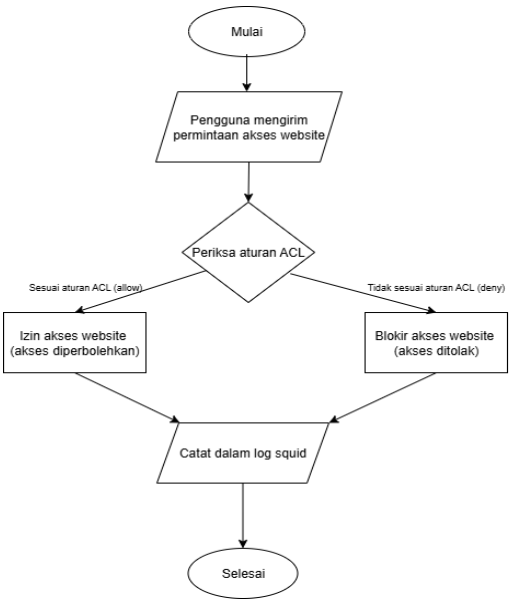

Figure 2. ACL Algorithm Flowchart

4. RESULT AND DISCUSSION

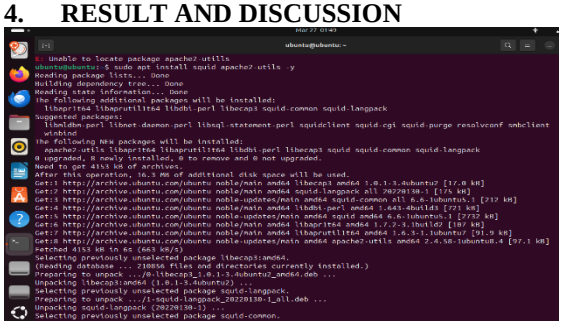

Figure 3. The First Stage

This figure illustrates the software installation process in Ubuntu, including how dependencies are managed automatically, as well as how apt works in downloading and installing packages from the official repositories. The installed squid package can be used as a caching proxy to improve internet access efficiency and control network traffic, while apache2-utils provides a variety of additional tools useful for Apache web server administrators.

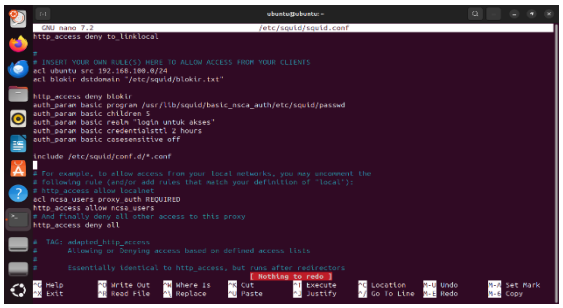

Figure 4. Second Stage

Squid is configured to strictly control internet access. Only logged-in users can use the proxy, and a list of blocked sites is maintained. With these settings, network administrators can ensure more controlled internet access, ensuring that not everyone can use the proxy freely, and that certain sites can be restricted according to their desired policies.

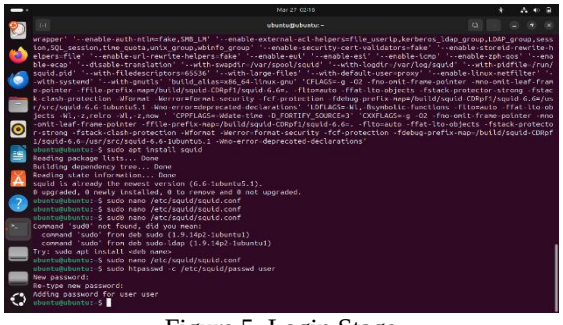

Figure 5. Login Stage

This process indicates that the user is setting up a Squid Proxy with a username and password authentication system. This is intended to restrict access to the proxy so that only users with the correct credentials can use it.

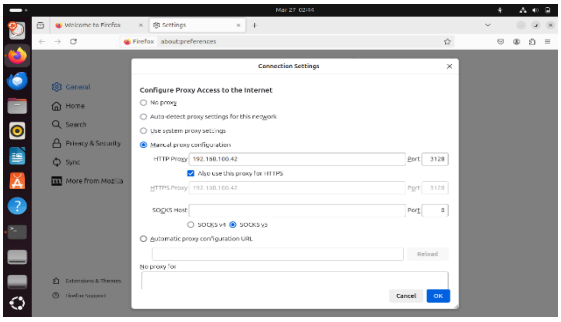

Figure 6. Configure Proxy

This image shows the connection settings in Firefox on the Ubuntu operating system, where the user is manually setting up proxy usage. In this setting, Firefox is directed to use a proxy with the address 192.168.100.42 and port 3128. The user also checked the "Also use this proxy for HTTPS" option, so that all HTTP and HTTPS connections will pass through this proxy. From this setting, it can be seen that Firefox will direct all its internet traffic through the proxy server 192.168.100.42:3128. This is the Squid Proxy, which can be used to control internet access, filter certain sites, or optimize network connections.

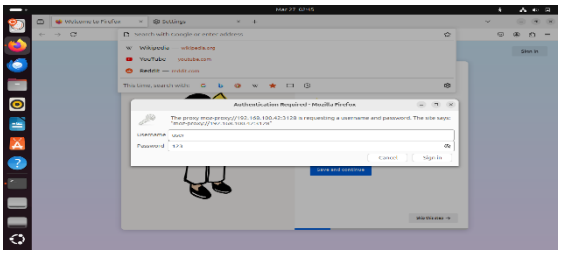

Figure 7. Enter Name And Password

In this image the user tries to access the Proxy by entering the username and password.

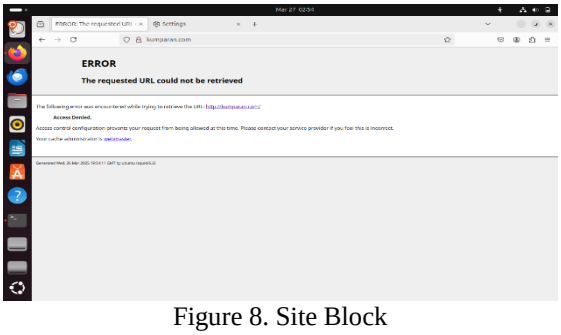

Figure 8. Site Block

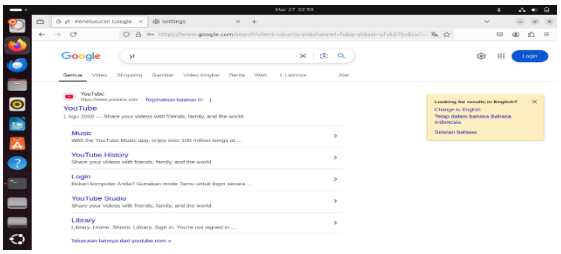

Figure 9. The Last

The image 8 shows that the blocked site cannot be opened again or displays an error. As shown in the image above, the user tries to open the blocked application (kumparan) and the result shows an error.

In the image 9, the user tries to open a website that is not blocked by the firewall and the result is successful.

Table 1. Website Blocking Test Results Using Squid Proxy

No	Website URL	Category	Access Attempt Result	Proxy Log Status	Description
1	www.facebook.com	Social Media	Blocked	TCP_DENIED/403	Successfully blocked by ACL rule.
2	www.youtube.com	Streaming	Blocked	TCP_DENIED/403	Access restricted according to policy.
3	www.wikipedia.org	Education	Allowed	TCP_MISS/200	Educational site — allowed.
4	www.twitter.com	Social Media	Blocked	TCP_DENIED/403	Filtering works as expected.
5	www.kemdikbud.go.id	Government	Allowed	TCP_HIT/200	Trusted government domain.
6	www.netflix.com	Streaming	Blocked	TCP_DENIED/403	Bandwidth-heavy site successfully blocked.

Table 1 shows the results of testing the website blocking feature using the Squid Proxy system. Each website was classified into categories such as social media, streaming, education, and government. The access attempt results indicate whether the website could be opened or was successfully blocked according to the Access Control List (ACL) configuration.

The Proxy Log Status column displays information from the Squid access.log file, where the code TCP_DENIED/403 indicates that access was denied, while TCP_MISS/200 or TCP_HIT/200 shows that access was permitted. The Description column provides brief notes confirming whether the filtering process worked according to the intended policy. Overall, the test demonstrates that the Squid Proxy is capable of effectively blocking non-educational or high-bandwidth websites, while still allowing access to useful and trusted resources.

5. CONCLUSION

The implementation of Squid Proxy as a firewall provides an effective solution for managing network security. This study revealed that Squid Proxy is capable of controlling internet access by implementing strict filtering policies, such as blocking sites deemed unsafe and only allowing access to authenticated users. Real-world implementations show that Squid Proxy not only functions as a tool for monitoring user activity but also helps prevent cyber threats such as data theft and malware distribution. Although Squid Proxy configuration and management require special attention to avoid negative impacts such as increased latency or unwanted access restrictions, test results indicate that this system has great potential for improving network security. This study also emphasizes the need for further evaluation and adjustment to optimize the performance and effectiveness of Squid Proxy-based firewalls, so that they can be adapted to the needs and security policies of each organization.

REFERENCE

[1] Z. Sitorus, dkk., “Blocking Prohibited Sites Using Proxy Server in Mikrotik and Squid Proxy Debian Server,” JITCSE, 2024.
[2] F. Ramaditia, A. Wijayanto, and A. Misbahuddin, “Monitoring dan Filtering Situs Pornografi pada Proxy Server Berbasis Naïve Bayes Classifier dan JADE,” TESLA, 2014.
[3] H. Husaini, M. Warisaji, and S. Saifudin, “Perbandingan Kinerja Pemblokiran Situs Porno Menggunakan Layer 7 Protocol dan Squid Proxy,” JUSTINDO, 2024.
[4] M. Kurniawan, dkk., “Implementasi Squid Proxy pada Mikrotik dan Monitoring Traffic Jaringan,” JATI, 2020.
[5] R. Rosihan and A. Apriyadi, “Perancangan Proxy Server dengan Menggunakan Squid,” Jurnal FT Informatika, 2017.
[6] D. A. Artika, dkk., “Mengimplementasikan Proxy Server (Squid) Berbasis Linux pada Ubuntu 22.04,” JATI, 2024.
[7] H. Gea, dkk., “Implementasi ACL untuk Monitoring Akses Jaringan Menggunakan Squid Proxy,” METHOMIKA, 2022.
[8] D. Dwiyatno, dkk., “Penerapan Internet Sehat Menggunakan Zabbix dan Squid Proxy,” IFTECH, 2021.
[9] J. Lin and C. Yao, “Firewall Anomaly Detection Based on Double Decision Tree,” Symmetry, 2022.
[10] B. Prasetyo, “Implementasi Manajemen Bandwidth dan Filtering Web Access Control Menggunakan Metode Address List,” JIKA (UMT), 2019