JURNAL SISTEM INFORMASI TGD
Volume 4, Nomor 6, November 2025, Hal 1328-1335
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Implementasi Content Filtering Pada Jaringan Internet Sekolah Dengan Autentikasi Data Siswa dan Squid Proxy

Muhammad Edi Iswanto[1], Robi Robianto[2], Willy Permana Putra[3], Joko Irawan[4], Renol Burjulius[5]
[1,2,4] Jurusan Teknik Informatika, Politeknik Negeri Indramayu
[2]Rekayasa Perangkat Lunak, Politeknik Negeri Indramayu
[5]Sistem Informasi Kota Cerdas, Politeknik Negeri Indramayu

Email: [1*]muhammad.edi@polindra.ac.id, [2]robiyanto@polindra.ac.id, [3]willy@polindra.ac.id, [4]joko_irawan@polindra.ac.id, [5]burjuliusrenol@gmail.com
Email Penulis Korespondensi: muhammad.edi@polindra.ac.id

Abstrak
Penelitian ini bertujuan untuk mengimplementasikan sistem content filtering pada jaringan internet sekolah menggunakan Squid Proxy yang terintegrasi dengan autentikasi pengguna melalui MikroTik. Permasalahan utama yang diangkat adalah maraknya akses terhadap konten negatif oleh siswa yang tidak sesuai dengan tujuan pembelajaran. Sistem dirancang dengan pendekatan transparan proxy agar tidak mengganggu kenyamanan pengguna. Hasil pengujian menunjukkan bahwa Squid Proxy mampu memblokir akses ke situs tertentu, terutama pada protokol HTTP, dengan menampilkan halaman peringatan yang sesuai. Namun, keterbatasan muncul pada protokol HTTPS, di mana halaman blokir tidak dapat ditampilkan karena enkripsi end-to-end. Selain itu, sistem belum mampu mengidentifikasi pengguna secara individual karena keterbatasan transparansi IP pada konfigurasi NAT di MikroTik. Sebagai alternatif, eksperimen tambahan dengan skenario explicit proxy menunjukkan potensi solusi untuk mengenali identitas pengguna, meskipun dengan konsekuensi konfigurasi yang lebih kompleks. Hasil penelitian ini diharapkan dapat menjadi rujukan bagi sekolah dalam menerapkan kontrol akses internet yang efektif dan edukatif.
Kata Kunci: Filtering, Internet, Mikrotik, Proxy, Squid

Abstract
This research investigates the implementation of a content filtering system within a school's internet network utilizing Squid Proxy, integrated with user authentication via MikroTik. The primary concern addressed in this study is the increasing exposure of students to inappropriate online content that contradicts educational objectives. The system is initially configured using a transparent proxy approach to ensure minimal disruption to user experience. Experimental results indicate that Squid Proxy is capable of effectively restricting access to specified websites, particularly those using the HTTP protocol, by displaying system-generated warning pages. Nonetheless, the system exhibits limitations in handling HTTPS traffic due to end-to-end encryption, which prevents the proxy from intercepting and displaying custom block notifications. Furthermore, the identification of individual users remains unachievable in this configuration, primarily due to IP address masking resulting from Network Address Translation (NAT) on the MikroTik router. To address these limitations, an additional experiment employing an explicit proxy scenario was conducted, which successfully enabled user-level identification, although requiring more intricate configuration. The findings of this research are intended to provide practical insights for educational institutions seeking to implement effective and pedagogically aligned internet access control mechanisms.
Keywords*: Filtering, Internet, Mikrotik, Proxy, Squid*

1. PENDAHULUAN

Dalam beberapa tahun terakhir, banyak sekolah di Indonesia telah mengadopsi infrastruktur jaringan lokal dengan akses internet nirkabel (Wi-Fi) guna mendukung proses belajar mengajar. Penyediaan koneksi internet yang stabil dan dapat diakses oleh seluruh civitas akademika merupakan salah satu bentuk adaptasi terhadap perkembangan teknologi informasi dan komunikasi (TIK), sekaligus upaya peningkatan kualitas pendidikan di era digital.

Implementasi jaringan Wi-Fi di lingkungan sekolah tidak hanya dimaksudkan untuk menyediakan konektivitas dasar, tetapi juga sebagai sarana peningkatan efisiensi pembelajaran berbasis digital. Penelitian yang dilakukan oleh Putro dan Iryanti [1] mengungkapkan bahwa pemanfaatan layanan WiFi Indibiz Pijar Sekolah secara signifikan dapat meningkatkan motivasi belajar siswa serta mendukung metode pembelajaran berbasis teknologi. Hal ini menjadi bukti bahwa kehadiran internet yang memadai di sekolah turut mempengaruhi kualitas proses pembelajaran.

Seiring meningkatnya kebutuhan terhadap layanan internet di sekolah, muncul pula kebutuhan manajerial untuk mengelola jaringan yang lebih baik. Salah satu aspek krusial adalah pengelolaan penggunaan jaringan oleh siswa agar tidak terjadi overload bandwidth dan penyalahgunaan akses. Studi yang dilakukan oleh Yuniant dan Setiyanti [2] menunjukkan bahwa penerapan sistem manajemen user, bandwidth, dan limit waktu pada jaringan hotspot Wi-Fi di lingkungan laboratorium sekolah berbasis perangkat Mikrotik dapat memberikan kontrol yang efisien terhadap penggunaan jaringan. Demikian pula, penelitian yang dilakukan oleh Aziz et al. [3] menerapkan sistem manajemen

JURNAL SISTEM INFORMASI TGD
Volume 4, Nomor 6, November 2025, Hal 1328-1335
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

jaringan berbasis aplikasi Mikhmon untuk memantau aktivitas pengguna secara real-time, termasuk data penggunaan bandwidth, durasi pemakaian, serta autentikasi nama pengguna. Hal serupa pernah diteliti oleh Asyifah dan Ramayanti [4] yang berhasil melakukan optimasi kinerja jaringan kinerja jaringan dengan memanfaatkan Mikrotik Rb 951ui-2hnd yang dipadukan Penerapan Algoritma Simple Queue untuk meningkatkan alokasi dan efisiensi bandwith sesuai dengan kebutuhan setiap ruangan di lingkungan SMK Al-Fudhola.

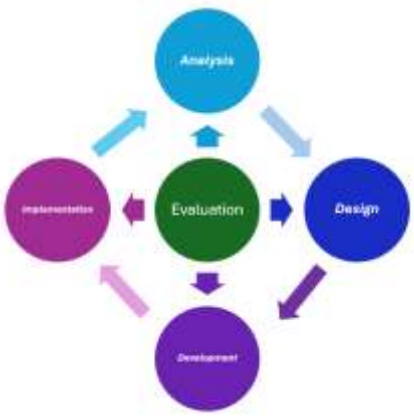
Di sisi lain, aspek keamanan jaringan juga menjadi perhatian penting dalam lingkungan pendidikan. Sekolah sebagai penyedia akses terbuka perlu memastikan bahwa jaringan yang disediakan tidak menjadi celah bagi tindakan penyalahgunaan atau ancaman siber. Penelitian oleh Eben et al. [5] menekankan urgensi penguatan sistem keamanan jaringan melalui konfigurasi firewall serta manajemen akses berbasis Router Mikrotik. Pendekatan ini terbukti meningkatkan stabilitas koneksi serta meminimalisir risiko serangan dari luar. Lebih jauh dari sekadar pengelolaan teknis, penyediaan layanan internet di sekolah perlu dibarengi dengan sistem penyaringan konten (content filtering) untuk menghindari akses terhadap konten negatif, seperti pornografi atau perjudian, yang dapat merusak moral dan konsentrasi siswa. Arrahman dan Widyassari [6] menunjukkan bahwa pengimplementasian Squid Proxy sebagai proxy server pada Debian mampu menyaring akses situs-situs tidak layak secara efektif, dengan hasil uji kelayakan sistem mencapai 100%. Walaupun dalam penelitian lain hal serupa dapat pula dilakukan dengan memanfaatkan layer 7 protocols seperti yang dilakukan oleh Shomat,et.al. [7] Yang berhasil melakukan pembatasan akses media sosial di SMK IDN, sehingga dapat memaksi siswa untuk dapat lebih bijak mengkases internet, yaitu dengan mengakses situs yang dianggap dapat menunjang proses belajar mengajar. Meskipun antara layer 7 protocols dan squid proxy dapat melakukan proses *filtering*, namun squid proxy dianggap lebih baik dibandingkan dengan layer 7 protocols, karena memiliki kecepatan load lebih baik baik dibandingkan dengan layer 7 protocols [8].

Berdasarkan beberapa kajian literatur dan fenomena di lapangan, mengindikasikan adanya kebutuhan akan sistem jaringan sekolah yang tidak hanya mengutamakan konektivitas dan efisiensi, tetapi juga menjamin aspek keamanan serta penggunaan internet yang bertanggung jawab. Oleh karena itu, penelitian ini mengusulkan suatu sistem jaringan internet sekolah yang mengintegrasikan proses autentikasi berbasis data siswa dengan mekanisme content filtering menggunakan Squid Proxy. Dalam sistem ini, autentikasi berfungsi sebagai gerbang awal untuk memastikan bahwa hanya siswa yang terdaftar secara resmi yang dapat mengakses jaringan internet. Setelah proses login berhasil, Squid Proxy kemudian berperan dalam memfilter aktivitas browsing siswa sesuai dengan kebijakan akses yang telah ditentukan. Pendekatan ini diharapkan mampu menciptakan ekosistem jaringan yang aman, terkontrol, dan sejalan dengan tujuan pembelajaran di lingkungan pendidikan.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Penelitian ini menggunakan metode Research and Development (R&D) yang bertujuan untuk menghasilkan produk sebuah sistem content filtering berbasis autentikasi data siswa di lingkungan sekolah. Metode ini memadukan proses riset dengan pengembangan produk secara sistematis, dimulai dari identifikasi kebutuhan hingga pengujian kelayakan sistem. R&D merupakan metode penelitian yang digunakan untuk menghasilkan produk tertentu dan menguji keefektifan produk tersebut [9], yang dalam proses penyelesaiannya, penelitian ini mengikuti tahapan yang terdapat pada model ADDIE seperti yang dapat dilihat pada Gambar 1.



Gambar 1. Tahap Penyelesaian Model ADDIE

ADDIE merupakan akronim dari *Analysis*, *Design*, *Development*, *Implementation*, dan *Evaluation* [10], yang menjadi karakteristik dalam proses penyelesaiannya. Berikut penjelasan dari setiap tahapan yang terdapat pada model ADDIE [10]:

a. *Analysis*, merupakan tahapan pertama yang dilakukan dalam model ADDIE, yang bertujuan untuk mengidentifikasi kebutuhan sistem, karakteristik pengguna, dan permasalahan utama yang terjadi. Dalam konteks ini ialah pemanfaatan jaringan internet di sekolah.

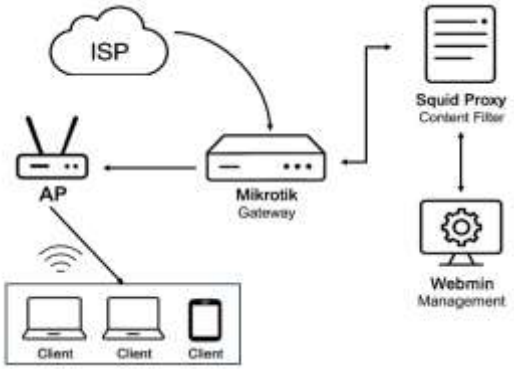
JURNAL SISTEM INFORMASI TGD
Volume 4, Nomor 6, November 2025, Hal 1328-1335
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

b. *Design*, ialah tahapan yang memfokuskan pada perancangan produk yang bersifat konseptual yang akan menjadi landasan utama pada tahapan berikutnya.
c. *Development*, tahapan ini adalah keberlanjutan dari tahap *design*, yaitu mengembangkan produk yang telah siap untuk diterapkan maupun diujicobakan. Pada tahap ini pula disusun instrumen yang bertujuan untuk mengukur kinerja sebuah produk.
d. *Implementation*, tahapan ini adalah fase pengimplementasian dari produk yang telah dikembangkan. Pada tahapan ini dihasilkan sebuah umpan balik berdasarkan instrumen yang telah disusun sebelumnya.
e. *Evaluation*, hasil umpan balik yang telah didapat, pada fase ini dinilai dan diukur untuk mengetahui ketercapaian dari produk atau model yang telah dikembangkan.

Model ini lebih sering digunakan dalam membantu pengembangan bahan ajar baik *onliine* maupun *offline*, seperti yang dilakukan oleh Rahmawati, et.al [11] yang memanfaatkan model ADDIE untuk mengembangkan e-modul pelatihan di Balai Diklat Keagamaan Surabaya. Meskipun demikian, model ini juga dapat digunakan dalam pengembangan sistem berbasis teknologi karena tahapannya yang bersifat sistematis dan iteratif. Sehingga mampu menghasilkan produk yang valid dan layak digunakan melalui tahap analisis kebutuhan hingga evaluasi produk secara menyeluruh [11]. Hal ini diperkuat dengan ilustrasi yang terlihat pada Gambar 1, dimana Setiap tahapan dilakukan evaluasi sebelum dilanjutkan ke tahapan berikutnya.

2.2 Arsitektur Sistem

Desain sistem *content filtering* dalam penelitian ini melibatkan Mikrotik sebagai gateway utama, Squid Proxy sebagai penyaring konten (*content filter*), dan Webmin sebagai antarmuka manajemen sistem. Struktur jaringan yang digunakan dapat dilihat pada Gambar 2.



Gambar 2. Desain Topologi Jaringan

Desain topologi yang diperlihatkan pada Gambar 2 menunjukkan koneksi internet dari *internet service provider* (ISP) diarahkan terlebih dahulu ke router Mikrotik yang berfungsi sebagai *gateway utama*. Seluruh perangkat klien, seperti laptop dan gawai siswa, terhubung ke jaringan melalui akses Wi-Fi yang dihasilkan oleh *Access Point* yang terhubung dengan Mikrotik.

Setiap klien diwajibkan melakukan login melalui sistem hotspot Mikrotik. Setelah proses autentikasi berhasil, trafik dari klien diarahkan ke server yang menjalankan layanan Squid Proxy. Squid bertugas menyaring permintaan akses berdasarkan daftar aturan (*Access Control List/ACL*) yang telah ditentukan, seperti pemblokiran terhadap situs-situs tidak relevan dengan kegiatan belajar.

Untuk mempermudah pengelolaan dan pemantauan sistem, layanan Squid Proxy dikonfigurasi dan diawasi menggunakan antarmuka Webmin. Webmin memungkinkan administrator jaringan melakukan pengelolaan layanan secara grafis, termasuk melihat log akses, mengatur ulang layanan, atau mengubah konfigurasi tanpa menggunakan *command line interface*.

Dengan integrasi ini, sistem mampu memberikan kontrol terhadap siapa yang dapat mengakses jaringan sekaligus membatasi konten yang dapat diakses oleh pengguna, sesuai kebijakan yang ditetapkan pihak sekolah.

2.3 Squid Proxy

Dilansir dari laman resminya, Squid Proxy merupakan perangkat lunak open source berlisensi GNU General Public License (GPL) yang berfungsi sebagai caching dan forwarding web proxy server. Squid mendukung berbagai protokol jaringan seperti HTTP, HTTPS, dan FTP, serta dapat dijalankan pada berbagai sistem operasi, khususnya platform berbasis Unix/Linux [12]. Sebagai salah satu jenis web proxy, Squid bekerja dengan menjadi perantara antara client dan server, di mana setiap permintaan dari klien akan diteruskan ke server tujuan melalui proxy. Mekanisme ini tidak hanya meningkatkan efisiensi penggunaan bandwidth dan kecepatan akses halaman web melalui caching, tetapi juga memungkinkan pengelolaan dan pengawasan aktivitas internet pengguna dalam suatu jaringan [13].

JURNAL SISTEM INFORMASI TGD
Volume 4, Nomor 6, November 2025, Hal 1328-1335
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

2.4 WebMin

Webmin merupakan sebuah *tools* berbasis web yang mensimplifikasi proses pengelolaan sistem linux atau unix dibandingkan dengan melakukan konfigurasi secara manual melalui Command Line Interface (CLI) [14]. Hal ini membuat pekerjaan mengelola sistem administrasi seperti mengatur pengguna, layanan jaringan, file sistem, firewall, hingga konfigurasi aplikasi server menjadi lebih mudah. Dalam penelitian ini, Webmin digunakan sebagai alat bantu visual untuk memantau dan mengelola konfigurasi server proxy, termasuk proses pengawasan log akses dan manajemen layanan jaringan secara real time.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Infrastruktur Jaringan Sekolah

Setelah melakukan analisis dan pengamatan tentang keadaan jaringan di lingkungan sekolah, langkah selanjutnya ialah merancang dan membangun infrastruktur dasar jaringan seperti yang dapat dilihat pada Gambar 2. Infrastruktur ini yang mengintegrasikan perangkat Mikrotik sebagai pengelola akses dan autentikasi, serta server lokal berbasis Linux Ubuntu yang menjalankan layanan *Squid Proxy*. Perangkat klien seperti laptop dan *gadget* siswa terhubung ke jaringan melalui jaringan nirkabel (Wi-Fi) yang disediakan oleh access point yang dikonfigurasi dari router Mikrotik.

Koneksi internet dari penyedia layanan (*Internet Service Provider/ISP*) diarahkan langsung ke perangkat Mikrotik, yang kemudian membagi trafik jaringan ke dua jalur utama, yaitu jalur untuk akses perangkat administrator jalur untuk trafik pengguna (siswa). Perangkat Mikrotik berperan sebagai *gateway* utama dan menyediakan layanan hotspot berbasis login. Autentikasi dilakukan agar hanya siswa yang memiliki akun resmi yang dapat terhubung ke internet.

Setelah proses login berhasil, trafik dari klien diarahkan ke server lokal yang menjalankan Squid Proxy. Untuk mendukung konfigurasi awal dan pemantauan sistem, server juga dilengkapi dengan antarmuka *Webmin* yang memungkinkan administrator untuk mengatur sistem dan melihat log akses secara real time. Secara umum struktur jaringan yang dibangun dibagi menjadi tiga segmen utama, yaitu:

a. Uplink, yaitu jalur dari ISP menuju Mikrotik.
b. Gateway, yakni Mikrotik sebagai pengatur login dan pengarah trafik.
c. Filtering & Monitoring, dengan Server Linux yang menjalankan Squid Proxy dan Webmin, serta menyimpan log aktivitas pengguna.

Implementasi infrastruktur ini dirancang untuk memenuhi kebutuhan jaringan yang aman dan terkendali di lingkungan sekolah. Pemisahan fungsi antar perangkat (router, proxy server, dan interface monitoring) bertujuan untuk meningkatkan skalabilitas dan kemudahan pengelolaan jaringan ke depannya. Selain itu, konfigurasi jaringan ini juga memungkinkan perluasan fungsi, seperti penerapan pembatasan waktu akses, pembagian bandwidth, serta pengintegrasian sistem notifikasi berbasis log jika dibutuhkan di masa mendatang.

3.2 Implementasi Squid Proxy dan WebMin

Setelah infrastruktur jaringan terimplementasi dengan baik, tahap selanjutnya adalah mengimplementasikan squid proxy sebagai inti dari pembahasan ini, yaitu *content filtering*. Squid proxy di install dan dijalankan pada serveer lokal berbasis Ubuntu 22.04. Hal pertama yang dilakukan setelah squid proxy berjalan, adalah melakukan beberapa konfigurasi dasar pada squid proxy melalui file squid.conf pada direktori /etc/squid. Beberapa konfigurasi tersebut meliputi:

a. Menentukan port layanan proxy. Port yang digunakan pada penelitian ini menggunakan port default dari squid proxy yaitu 3128.
b. Menentukan jaringan lokal yang diizinkan mengakses layanan proxy. Proses ini bertujuan untuk menambahkan port default dari webmin yaitu 10000, dengan tujuan memastkan akses administrator tidak terganggu.
c. Mengatur kebijakan akses melalui direktif http_access. Pada proses ini dideklarasikan pula sebuah parameter seperti yang terdapat pada Gambar 3, yaitu menambahkan sebuah file dengan nama blocked_sites. File ini berisi daftar domain yang tidak dizinkan seperti yang dapat dilihat pada Gambar 4. Dengan konfigurasi ini, setiap permintaan akses ke domain yang tercantum dalam daftar akan secara otomatis ditolak oleh Squid.

```
acl blocked_sites dstdomain "/etc/squid/blocked_sites"
http_access deny blocked_sites
```

Gambar 3. Script Untuk Penyaringan Content

```
 GNU nano 6.2                          /etc/squid/blocked_sites
facebook.com
tiktok.com
www.youtube.com
chatgpt.com
tv6.lk21official.cc
rebahinxxi1.today
```

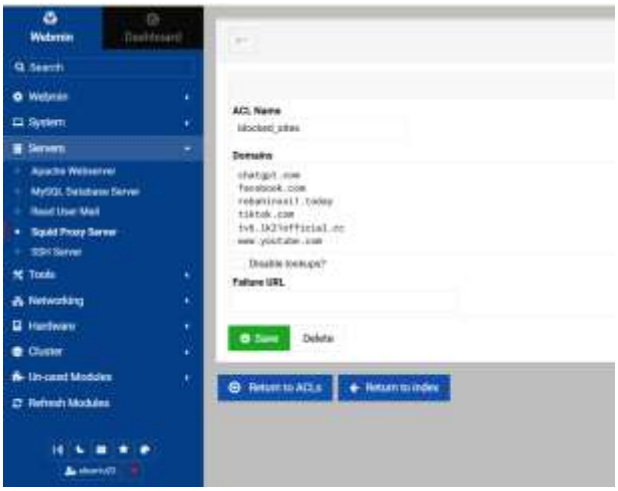
JURNAL SISTEM INFORMASI TGD
Volume 4, Nomor 6, November 2025, Hal 1328-1335
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Gambar 4. Isi file blocked_sites

Untuk memudahkan proses administrasi dan pemantauan sistem, server juga dilengkapi dengan *Webmin*, yaitu antarmuka web berbasis GUI yang memungkinkan administrator melakukan berbagai konfigurasi sistem, melihat log, serta mengelola layanan tanpa perlu mengakses terminal secara langsung. Webmin dijalankan melalui port 10000 yang sebelumnya telah ditambahkan dalam daftar pengecualian akses agar tidak terkena pemblokiran oleh proxy sehingga akan menampilkan halaman dashbord WebMin seperti pada Gambar 5.

Gambar 5. Dashbord WebMin

Seperti yang terlihat pada Gambar 5, terdapat banyak modul yang disediakan oleh WebMin untuk memudahkan dalam proses administrasi server, namun salah satu modul yang akan digunakan pada peneltian ini adalah modul *Squid Proxy Server* yang terdapat pada tab servers. Dalam modul tersebut memungkinkan administrator melihat dan mengelola konfigurasi Squid, termasuk daftar domain yang diblokir secara langsung melalui antarmuka web. Termasuk di dalamnya adalah menambahkan atau menghapus domain dalam daftar blokir seperti yang dapat dilihat pada Gambar 6, memuat ulang konfigurasi Squid tanpa akses terminal, dan melihat status layanan proxy secara real-time melalui menu systems logs dengan sedikit melakukan modifikasi yakni menambahkan perintah menuju direktori /var/log/squid/access.log seperti yang dapat dilihat pada Gambar 7.



Gambar 6. Mengelola daftar domain melalui WebMin

JURNAL SISTEM INFORMASI TGD
Volume 4, Nomor 6, November 2025, Hal 1328-1335
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Gambar 7. Log Layanan Proxy

Melalui Webmin proses konfigurasi dan pemantauan sistem menjadi lebih praktis dan efisien, terutama bagi operator jaringan di lingkungan sekolah yang mungkin belum terbiasa dengan antarmuka terminal berbasis perintah. Tahap implementasi ini memastikan bahwa sistem filtering dapat dikendalikan dan dimodifikasi dengan mudah sesuai kebutuhan kebijakan sekolah. Selanjutnya, proses pengujian dan evaluasi akan dijelaskan secara rinci pada subbab berikutnya.

3.3 Pengujian dan Evaluasi Sistem

Setelah Squid Proxy sebagai mesin utama dalam *content filtering* dan WebMin sebagai *interface* administrasi telah terimplementasi dengan baik, tahap selanjutnya adalah memastikan sistem *content filtering* berjalan secara menyeluruh melalui integrasi dengan perangkat jaringan MikroTik. Untuk mengimplemntasikan hal tersebut, dilakukan konfigurasi NAT (*Network Address Translation*) pada router MikroTik melalui pendekatan dst-nat seperti yang dapat dilihat pada Gambar 8. Dengan metode tersebut, seluruh trafik yang masuk melalui port 80 (HTTP) dari interface ether3-HotSpot1 akan dialihkan secara otomatis ke alamat IP server Squid yaitu 192.168.8.31 pada port 3128. Port ini merupakan port alternatif Squid yang telah diatur secara khusus untuk menerima trafik transparan proxy.

Gambar 8. Konfigurasi NAT pada Mikrotik

Pada tahap pengujian, sistem berhasil menyaring akses ke domain yang telah ditambahkan ke dalam daftar blokir, yang menunjukkan bahwa sistem sudah menunjukkan kinerja yang baik, terutama ketika mengakses domaian dengan protokol HTTP yang dimasukkan kedalam daftar blokir, maka akan ditampilkan secara eksplisit halaman error dari squid proxy seperti yang ditunjukkan pada Gambar 9.

Gambar 9. Halaman Error Squid Proxy Untuk Protokol HTTP

JURNAL SISTEM INFORMASI TGD
Volume 4, Nomor 6, November 2025, Hal 1328-1335
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Namun, hal berbeda ketika domain yang dimasukkan kedalam daftar blokir memiliki protokol HTTPS, maka tidak akan ditampilkan pesa error serupa, melainkan peringatan seperti pada Gambar 10 ketika diakses melalui browser Google Chrome, maupun Gambar 11 ketika di akses melalui browser Firefox. Hal ini disebabkan karena Protokol HTTPS dirancang dengan enkripsi *end-to-end encryption*, sehingga komunikasi antara klien dan server tujuan tidak dapat dibaca ataupun dimodifikasi oleh pihak ketiga [15], termasuk didalamnya proxy yang berada di tengah jalur komunikasi. Oleh karena itu, Squid tidak dapat menyisipkan atau mengganti halaman yang ditampilkan kepada pengguna ketika situs HTTPS diblokir.

Gambar 10. Halaman Error Squid Proxy Untuk Protokol HTTPS Pada Chrome

Gambar 11. Halaman Error Squid Proxy Untuk Protokol HTTPS Pada Firefox

Kondisi lain yang menjadi kendala adalah ketidakmampuan sistem untuk mengenali identitas pengguna secara individu seperti yang terlihat pada Gambar 7. Seluruh trafik yang tercatat dalam log squid berasal dari satu alamat IP yang saman, yakni IP dari MikroTik sebagai *gateway*. Hal ini menjadi penghambat dalam penerapan kebijakan penyaringan berbasis identitas pengguna, seperti berdasarkan alamat IP atau username hasil autentikasi login. Dampaknya, sistem tidak dapat melakukan tindak lanjut atau pencatatan spesifik terhadap pengguna yang mencoba mengakses situs yang diblokir, meskipun sebelumnya telah melakukan login melalui halaman hotspot MikroTik.

Berdasarkan hasil pengujian yang telah dilakukan, sistem content filtering yang mengintegrasikan Squid Proxy dengan MikroTik telah mampu menyaring akses terhadap domain yang masuk dalam daftar blokir, terutama pada protokol HTTP. Namun demikian, sistem ini masih memiliki beberapa keterbatasan, seperti menampilkan pesa blokir yang kurang informatif ketika terjadi pemblokiran pada situs dengan protokol HTTPS. Selanjutnya adalah ketidakmampuannya dalam membedakan identitas pengguna secara individu, yang dalam konteks lingkungan pendidikan, kemampuan untuk memantau dan mengatur akses berdasarkan identitas pengguna menjadi sangat penting, baik untuk pembinaan maupun untuk pelaporan. Ketika sistem tidak mampu membedakan pengguna satu dengan yang lain, maka potensi pelanggaran terhadap kebijakan akses tidak dapat ditindak secara spesifik. Ini mengurangi nilai strategis dari sistem filtering sebagai alat pendukung manajemen akses berbasis kontrol identitas.

Sebagai bentuk pengayaan terhadap penelitian utama, dilakukan eksperimen tambahan dalam lingkungan laboratorium sekolah dengan menggunakan skenario *explicit proxy*, sebagaimana yang telah diterapkan oleh Arrahman dan Widyassari [6] di SMK Al Muhammad Cepu. Pada pendekatan ini, dilakukan konfigurasi secara manual pada perangkat klien untuk menggunakan Squid Proxy, yaitu dengan mengarahkan koneksi ke alamat IP server proxy melalui port 3128. Dengan metode ini, server proxy mampu mengenali alamat IP atau identitas dari pengguna. Meskipun menawarkan keunggulan dalam hal pencatatan dan kontrol akses berbasis identitas pengguna, pendekatan ini memiliki keterbatasan dalam hal skalabilitas karena memerlukan konfigurasi individual pada setiap perangkat. Sebagai alternatif lain, fitur tproxy pada kernel Linux dapat digunakan untuk mempertahankan mode transparan sambil tetap meneruskan IP asli klien. Namun, fitur ini belum dapat diimplementasikan dalam penelitian ini karena keterbatasan dukungan kernel pada perangkat yang digunakan.

JURNAL SISTEM INFORMASI TGD
Volume 4, Nomor 6, November 2025, Hal 1328-1335
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

4. KESIMPULAN

Penelitian ini telah berhasil mengimplementasikan sistem *content filtering* pada jaringan internet sekolah dengan mengintegrasikan Squid Proxy sebagai filter utama, WebMin sebagai antarmuka administrasi, serta perangkat MikroTik sebagai pengatur lalu lintas jaringan. Sistem yang dikembangkan mampu menyaring akses terhadap situs yang termasuk dalam daftar blokir, khususnya untuk protokol HTTP. Konfigurasi transparent proxy melalui metode dst-nat pada MikroTik memungkinkan seluruh trafik dialihkan secara otomatis ke server proxy tanpa memerlukan konfigurasi manual pada sisi klien, sehingga mempermudah penerapan dalam skala jaringan umum.

Meskipun sistem telah berfungsi dengan baik dalam menyaring akses berbasis domain, terdapat beberapa keterbatasan yang ditemukan selama pengujian. Salah satunya adalah ketidakmampuan sistem untuk menyaring situs yang menggunakan protokol HTTPS secara eksplisit, karena sifat enkripsi end-to-end yang membatasi kemampuan proxy untuk menyisipkan pesan atau halaman blokir. Selain itu, identitas pengguna tidak dapat dikenali secara individu karena semua trafik yang diteruskan dari MikroTik ke Squid hanya menampilkan alamat IP gateway, sehingga membatasi kemungkinan penerapan kebijakan penyaringan yang lebih personal atau berbasis identitas pengguna.

Meskipun tidak menjadi fokus utama, eksperimen tambahan dengan pendekatan explicit proxy di lingkungan terbatas yang dalam hal ini adalah laboratorium sekolah, menunjukkan potensi solusi untuk mengatasi keterbatasan identifikasi pengguna, meskipun dengan konsekuensi tambahan dalam hal konfigurasi.

UCAPAN TERIMAKASIH

Penelitian ini didanai oleh Pusat Penelitian dan Pengabdian Kepada Masyarakat (P3M), Politeknik Negeri Indramayu melalui Kegiatan PUKTI 2025 Nomor: 0665/PL42.PL42.9/AL.04/2025

DAFTAR PUSTAKA

[1] Mohammad Satrio Eko Putro and Endang Iryanti, "PENGGUNAAN WIFI INDIBIZ UNTUK MENUNJANG AKTIVITAS BELAJAR MENGAJAR DI SEKOLAH DASAR WILAYAH WARU," *Bhakti Nagori (Jurnal Pengabdi. Kpd. Masyarakat)*, vol. 5, no. 1, pp. 19–25, 2025, doi: https://doi.org/10.36378/bhakti_nagori.v5i1.3998.

[2] Misael Yuniant and Angela Atik Setyani, "MANAJEMEN USER, BANDWIDTH DAN LIMIT TIME HOTSPOT WIFI LAB MENGGUNAKAN MIKROTIK," *J. Pendidik. Teknol. Informasti*, vol. 2, no. 6, pp. 367–380, 2023, doi: https://doi.org/10.37792/jukanti.v6i2.1053.

[3] Filzam Ulil Aziz, Anang Efendi, and Robiatul Adawiyah, "Penerapan Sistem Hotspot Wifi Pengguna Internet Menggunakan Mikhmon Dan Mikrotik (Studi Kasus Pada SMP Pomosda, Tanjunganom, Nganjuk)," *J. Apl. Sist. dan Tek. Inform. Pomos.*, vol. 2, no. 1, pp. 9–15, 2024, [Online]. Available: https://jurnal.stt-pomosda.ac.id/index.php/jastip/article/view/139

[4] Nurul Asyifah and Desi Ramayanti, "Optimasi Kinerja Jaringan Di Smk Al Fudhola Bekasi: Pengaturan Bandwidth Dengan Mikrotik Rb 951ui-2hnd Dan Penerapan Algoritma Simple Queue," *J. Ilm. Ilk.*, vol. 7, no. 1, pp. 33–46, 2024, doi: https://doi.org/10.47324/ilkominfo.v7i1.210.

[5] Eben, Mukramin, and Hisma Abduh, "PENGEMBANGAN MANAJEMEN KEAMANAN JARINGAN NIRKABEL (WIFI) MENGGUNAKAN ROUTERBOARD MIKROTIK DAN FIREWALL PADA SMK KRISTEN PALOPO," *J. Inform. dan Tek. Elektro Terap.*, vol. 3, no. 12, 2024, doi: https://doi.org/10.23960/jitet.v12i3.4716.

[6] Riski Nur Arrahman and Adhika Pramita Widyassari, "Implementasi Proxy Server Sebagai Content Filtering Menggunakan Linux Debian Buster," *J. Ilm. IntechInformation Technol. J. UMUS*, vol. 4, no. 1, pp. 76–86, 2022, doi: https://doi.org/10.46772/intech.v4i01.677.

[7] Abdul Shomad, Yuma Akbar, and Dadang Iskandar Mulyana, "Implementasi Pembatasan Akses Sosial Media Menggunakan Layer 7 Protocol Pada Perangkat Mikrotik DI SMK IDN," *INFORMATICS Educ. Prof. J. INFORMATICS*, vol. 7, no. 1, pp. 27–38, 2022, doi: https://doi.org/10.51211/itbi.v7i1.1998.

[8] Moh Husaini, Taufiq Timur Warisaji, and Ilham Saifudin, "Perbandingan Kinerja Pemblokiran Situs Porno Menggunakan Layer 7 Protocol dan Squid Proxy," *JUSTINDO (jurnal Sist. dan Teknol. Inf. Indones.*, vol. 9, no. 1, pp. 10–16, 2024, doi: https://doi.org/10.32528/justindo.v9i1.981.

[9] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung: CV. Alfabeta, 2013.

[10] Marinu Waruwu, "Metode Penelitian dan Pengembangan (R&D): Konsep, Jenis, Tahapan dan Kelebihan," *J. Ilm. Profesi Pendidik.*, vol. 9, no. 2, pp. 1220–1230, 2024, doi: https://doi.org/10.29303/jipp.v9i2.2141.

[11] Fenny Rahmawati, Ibut Priono Leksono, and Ujang Rohman, "Pengembangan E-Modul Mata Pelatihan Pemetaan Kompetensi dan Indikator Berbasis Flip PDF Corporate Edition dengan Menggunakan Model ADDIE pada Pelatihan Metodologi Pembelajaran di Balai Diklat Keagamaan Surabaya," *EDUKASIA J. Pendidik. dan Pembelajaran*, vol. 4, no. 2, pp. 1647–1656, 2023, doi: https://doi.org/10.62775/edukasia.v4i2.469.

[12] https://www.squid-cache.org/, "Squid: Optimising Web Delivery." Accessed: Jun. 29, 2025. [Online]. Available: https://www.squid-cache.org/

[13] Heru Kurniawan, Josep Dedy Irawan, and FX. Ariwibisono, "Implementasi Squid Proxy Pada Mikrotik Dan Monitoring Traffic Jaringan Berbasis Website," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 4, no. 2, pp. 136–143, 2020, doi: https://doi.org/10.36040/jati.v4i2.2691.

[14] Jamie Cameron, "What is Webmin?," https://webmin.com/docs/intro/. [Online]. Available: https://webmin.com/docs/intro/

[15] "What is HTTPS?" Accessed: Jul. 05, 2025. [Online]. Available: https://www.cloudflare.com/learning/ssl/what-is-https/