

---

## IMPLEMENTASI METODE ACCESS CONTROL LIST UNTUK MEMONITORING AKSES JARINGAN MENGGUNAKAN SQUID PROXY

Asaziduhu Gea<sup>✉</sup>, Mufria J. Purba, Alfonso A. Putra, Jamaluddin, Rimbun Siringoringo

Universitas Methodist Indonesia, Medan, Indonesia

Email: [gea.asaziduhu@gmail.com](mailto:gea.asaziduhu@gmail.com)

DOI: <https://doi.org/10.46880/jmika.Vol6No1.pp79-84>

### ABSTRACT

*There is no doubt that technological advances, many can be done easily without having to go through a long process. For example, by utilizing a network connection in various ways. Like looking to collect and get data whether it's using a LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network). This application mentions that every user who wants to use the Internet must register with the Administrator by using the Mac Address on the device. So, not too many devices are connected to the network so that it makes an Internet network. The results showed that the implementation of monitoring network access using a squid proxy using the standard access control list implementation method was able to minimize leakage of internet bandwidth usage and limit users so that internet access was more secure.*

**Keyword:** *Squid, Proxy, Access Control List.*

### ABSTRAK

Kemajuan teknologi sudah tidak diragukan lagi, Banyak yang bisa dilakukan dengan mudah tanpa harus melewati proses yang panjang. Contohnya saja dengan memanfaatkan koneksi jaringan dalam berbagai hal. Seperti mencari mengumpulkan dan mendapatkan data baik itu menggunakan jaringan LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network). Aplikasi ini menyebutkan bahwa setiap user yang ingin menggunakan Internet harus mendaftar ke Administrator dengan menggunakan Mac Address pada perangkat. Sehingga, tidak terlalu banyak perangkat yang terhubung kepada Jaringan sehingga membebani jaringan Internet. Hasil penelitian menunjukkan bahwa dengan implementasi monitoring akses jaringan menggunakan squid proxy dengan menggunakan metode implementasi standard access control list mampu meminimalisir kebocoran penggunaan bandwidth internet dan membatasi pengguna sehingga akses internet lebih terjaga.

**Kata Kunci:** *Squid, Proxy, Access Control List.*

---

### PENDAHULUAN

Penggunaan koneksi internet yang semakin meluas dan meningkatnya transaksi bisnis lewat layanan internet, mendorong setiap pengguna untuk mengamankan transkasinya. Ada banyak metode yang diimplementasikan salah satunya ialah dengan mengimplementasikan squid proxy server (Kurniwan, 2012). Squid ialah proxy server yang memiliki kemampuan yang sangat baik. Selain dapat membagi akses internet kepada banyak user dan merecord aktivitas user pada cache, squid juga dapat mengelola jalur lalu lintas permintaan data dari user ke internet dan membatasinya jika dibutuhkan. Pengelolaan tersebut terkadang diperlukan dan kerena manfaat internet secara bersama-sama seringkali tidak maksimal penggunaannya. Lalu lintas permintaan data dari internet untuk setiap pengguna tidak diatur berdasarkan kebutuhan dan kondisi bandwidth yang mereka miliki. Setiap pengguna bisa mendapatkan hak

akses internet sesuai dengan bidang pekerjaannya atau kebutuhan yang seharusnya didapatkan. Selain itu, orang yang tidak memiliki akses atas hak penggunaan internet juga bisa dicegah (Maulana & Erlansyah, 2017).

Server proxy merupakan server komputer yang memiliki kemampuan untuk bertindak sebagai komputer lain dengan merequest konten dari internet atau intranet. Proxy server bertindak sebagai gateway ke dunia maya (internet) untuk setiap komputer klien. Sebenarnya server proxy tidak terlihat oleh komputer klien (Khasanah, 2017). Jika pengguna berinteraksi dengan internet melalui server proxy, klien tidak akan tahu bahwa server proxy-lah yang menangani permintaan tersebut. Web server yang menerima request dari proxy server akan menginterpretasikan request tersebut seolah-olah request tersebut datang langsung dari komputer client, bukan dari proxy server. Sebuah server proxy memiliki fungsi lebih dari sebuah

router yang memiliki fitur packet filtering karena merupakan server proxy yang beroperasi pada tingkat yang lebih tinggi dan memiliki kontrol yang lebih menyeluruh atas akses jaringan (Purwanto, Kusriani, & Huizen, 2017). Sebuah server proxy yang berfungsi sebagai "agen keamanan" untuk jaringan pribadi, umumnya dikenal sebagai firewall. Access list adalah pengelompokan paket berdasarkan kategori.

Daftar akses bisa sangat membantu ketika Anda membutuhkan kontrol atas lalu lintas jaringan. Daftar akses adalah alat pilihan untuk pengambilan keputusan dalam situasi ini. Penggunaan daftar akses yang paling umum dan paling mudah dipahami adalah memfilter paket yang tidak diinginkan saat menerapkan kebijakan keamanan (Laksono & Nasution, 2020). Kita dapat mengatur daftar akses untuk membuat keputusan yang spesifik tentang aturan pola lalu lintas sehingga daftar akses hanya mengizinkan host tertentu untuk mengakses hostname dengan WWW sementara yang lain tidak diizinkan (Ritonga, Saragih, & Gea, 2020). Dengan kombinasi daftar akses yang tepat, manajer jaringan memiliki kendali untuk menerapkan kebijakan terkait keamanan yang dibuat (Hafizhan, Wahyuddin, & Komalasari, 2020).

Dalam penelitian ini akan dibahas konsep kontrol akses yang dilakukan oleh Access Control List pada server proxy squid, disertai dengan contoh implementasi Access Control List. Untuk dapat mengakses jaringan nirkabel, setiap perangkat komputer harus mendaftarkan alamat Media Access Control List (MAC)-nya kepada administrator yang nantinya akan dimasukkan ke dalam Access Control List yang diatur pada server proxy Squid. Selain MAC Address, penelitian ini juga akan menambahkan parameter lain dalam proses otorisasi seperti IP filtering, Device Restrictions, dan User Authentication. Access Control List nantinya akan berfungsi untuk memberikan kewenangan kepada perangkat komputer yang akan terhubung dengan jaringan yang ada.

Tujuan dari perancangan sistem ialah untuk menerapkan filter pada Pengguna komputer khususnya yang terkoneksi di internet di Lingkungan Dinas Kependudukan dan Pencatatan Sipil Toba Samsuir, Mengontrol Arus lalu lintas Jaringan, Pemantauan log Akses, Pembatasan Device pada User, User menggunakan User dan Password ketika Login. Selain itu penelitian ini juga sebagai sarana pembelajaran tentang pengendalian penggunaan system sharing internet dan keamanan jaringan computer untuk penggunaan internet, Mengurangi kepadatan lalu lintas jaringan internet, Membatasi device pada

lingkungan Dinas Kependudukan dan Pencatatan Sipil Kabupaten Toba Samsuir.

Ada banyak penelitian yang terkait dengan keamanan akses data, salah satunya tentang Implementasi firewall didalam jaringan komputer. Seperti diberitakan media massa pada 12 Mei 2015 bahwa Indonesia merupakan negara asal kejahatan siber terbesar kedua di dunia (Permana, 2015). Lebih lanjut, laporan yang dikeluarkan pada tahun 2014 oleh Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (id-SIRTII) menyebutkan terdapat ± 350.000 serangan pada bulan Mei dalam bentuk exploit (Direktorat Operasi Keamanan Siber, 2014). Eksploitasi adalah kode yang secara khusus menyerang keamanan komputer. Eksploitasi banyak digunakan untuk penetrasi, baik secara legal maupun ilegal untuk menemukan kerentanan pada komputer target.

Selain itu, penelitian terkait pemanfaatan jalur komunikasi dalam jaringan secara maksimal merupakan faktor utama yang harus diperhatikan serta pengelolaannya, baik hak akses pengguna maupun waktu akses yang diberikan. Terkait keamanan dan kenyamanan juga menjadi faktor yang perlu diperhatikan. Squid adalah salah satu software proxy terbaik yang biasa digunakan sebagai proxy caching engine untuk Web Client, seperti HTTP, HTTPS, FTP, Gopher dan layanan sejenis lainnya, dengan Squid juga mampu mengurangi konsumsi bandwidth sekaligus mempercepat waktu respon karena ke halaman web yang belum pernah digunakan sebelumnya dikunjungi tidak perlu dipanggil kembali semuanya disimpan dalam proxy caching yang menghasilkan waktu akses yang lebih cepat (Hafizh, 2011).

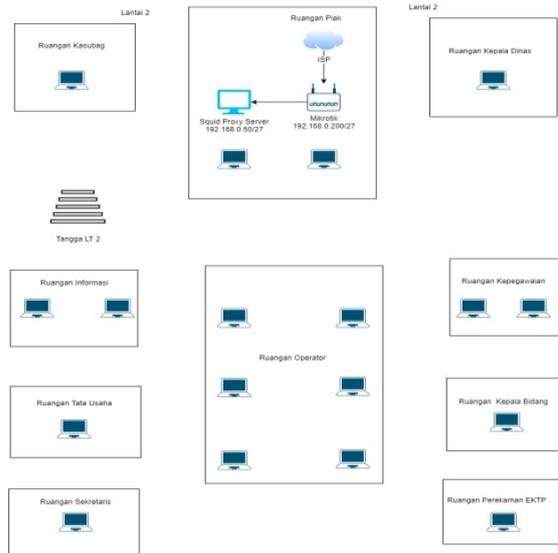
## **METODOLOGI DAN PERANCANGAN**

### **Perancangan Skema Jaringan Usulan**

Dari analisis skema jaringan yang lama, maka penulis mengusulkan sebuah skema jaringan yang baru. Pada rancangan yang diusulkan adalah dengan menambahkan sebuah server proxy yang berfungsi untuk mengontrol pemakaian bandwidth serta pengaksesan situs. Rancangan dibuat dengan mengelompokkan group user sesuai dengan tingkat kebutuhannya akan sumber daya internet.

Pada gambar tersebut memiliki beberapa interface, dimana interface berfungsi untuk menghantarkan layanan internet dari ISP ke komputer server, interface berikutnya untuk meneruskan layanan internet dari interface sebelumnya kepada client-client. Dari rancangan tersebut sumber daya internet akan

terdistribusikan secara merata kepada client-client tanpa adanya daya tarik menarik bandwidth antar user.



Gambar 1. Skema Jaringan Usulan

**Analisis Perangkat Jaringan**

Dinas Kependudukan dan Pencatatan Sipil Kabupaten, Toba Samosir memiliki komputer yang cukup banyak dalam mengerjakan/melaksanakan setiap tugas dan fungsi masing-masing sub bagian dan seksi yang ada. Jaringan komputer pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten, Toba Samosir pada dasarnya digunakan untuk membantu pertukaran data dan informasi setiap sub bagian, terutama untuk mengakses ke jaringan Internet.

Usulan biaya merupakan hitungan perkiraan biaya yang nantinya akan dipakai untuk menjalankan suatu proyek. Karena itu perlu perencanaan anggaran untuk mengetahui besaran biaya yang diperlukan. Perencanaan diperlukan untuk memprediksi biaya yang dikeluarkan agar perencanaan keuangan menjadi lebih terarah. Untuk mempermudah, maka dapat digunakan catatan dengan terorganisir. Untuk membangun Infrastrukturnya yang diperlukan hanyalah Server dan Mikrotik.

Tabel 1. Infrastruktur Biaya

Komputer	Normal	
Processor	Intel Core-I5	= Rp. 1.500.00
RAM	8 Gb	= Rp. 650.000
HDD	500 Gb	= Rp. 600.000
Vga:750	2 GB	= Rp. 1.000.000
Mikrotik	Rb941	= Rp. 350.000
Wifi	Rp. 450.000/Bulan Dengan 30 Mbps	

**Konfigurasi IP Address**

Penyelesaian pada perangkat sesuai topologi dimana setting IP Address PC Client, IP Address=DHCP dengan mapping IP Address untuk lokal seperti yang terlihat pada Tabel. IP address ini setiap host yang terhubung ke jaringan berbasis TCP/IP. Alamat IP dapat diasumsikan sebagai sebuah alamat.

Tabel 2. IP Address

192.168.200.1/24	192.168.200.0	Local
182.168.100.2/24	192.168.100.0	Wan
10.10.10.1/27	10.10.10.0	Wifi
192.168.0.200	192.168.0.0	Proxy

**Konfigurasi Subnetting /27 Client**

Dari subnet /27 Client, maka dari 32 bits alamat IP, 27 bits dialokasikan untuk network-id, tersisa 5 bits untuk host-id jumlah alamat IP yang ada dalam subnet.

Tabel 3. Subnetting /27 Client

IP Address	Netmask	Broadcast
10.10.10.2/27	255.255.255.224	10.10.10.31
10.10.10.3/27	255.255.255.224	10.10.10.31
10.10.10.4/27	255.255.255.224	10.10.10.31
10.10.10.5/27	255.255.255.224	10.10.10.31
10.10.10.6/27	255.255.255.224	10.10.10.31
10.10.10.7/27	255.255.255.224	10.10.10.31
10.10.10.8/27	255.255.255.224	10.10.10.31
10.10.10.9/27	255.255.255.224	10.10.10.31
10.10.10.10/27	255.255.255.224	10.10.10.31
10.10.10.11/27	255.255.255.224	10.10.10.31
10.10.10.12/27	255.255.255.224	10.10.10.31
10.10.10.13/27	255.255.255.224	10.10.10.31
10.10.10.14/27	255.255.255.224	10.10.10.31
10.10.10.15/27	255.255.255.224	10.10.10.31
10.10.10.16/27	255.255.255.224	10.10.10.31
10.10.10.17/27	255.255.255.224	10.10.10.31
10.10.10.18/27	255.255.255.224	10.10.10.31
10.10.10.19/27	255.255.255.224	10.10.10.31
10.10.10.20/27	255.255.255.224	10.10.10.31
10.10.10.21/27	255.255.255.224	10.10.10.31
10.10.10.22/27	255.255.255.224	10.10.10.31
10.10.10.23/27	255.255.255.224	10.10.10.31
Host : 30		

**Konfigurasi Routing**

Komputer yang berada pada jaringan 192.168.200.0/24 hanya dapat terhubung langsung dengan jaringan 192.168.200.0/24. Apabila komputer pada jaringan 192.168.200.0/24 ingin berkomunikasi

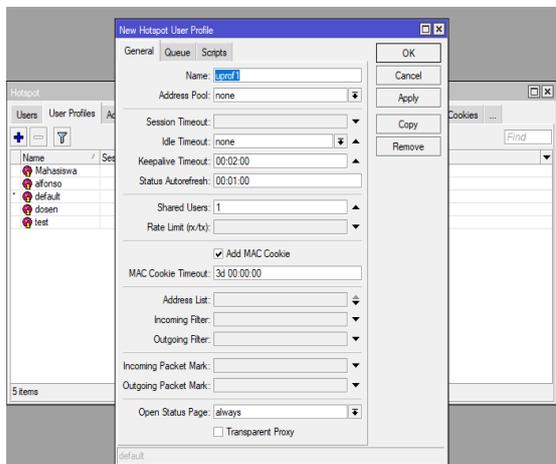
dengan komputer yang berada pada jaringan 192.168.100.0/24, maka harus melewati router.

**Tabel 4.** Routing

192.168.200.0/24	192.168.200.1
10.10.10.0/27	10.10.10.1
192.168.0.0	192.168.0.200
192.168.100.0	192.168.100.2

**Konfigurasi User Profile**

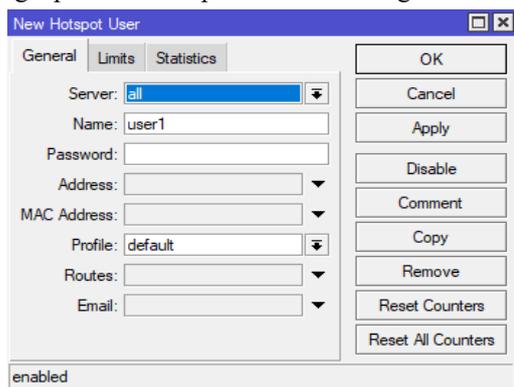
Konfigurasi user profile dapat dipakai untuk merecord konfigurasi-konfigurasi umum dari user-user hotspot. Profile ini dipakai untuk menggabungkan beberapa user. Hotspot user merupakan user yang dapat dipakai untuk login hotspot. Dalam sebuah jaringan dibutuhkan sebuah mekanisme pengaturan bandwidth (limit) yang bertujuan mencegah terjadinya monopoli pemakaian bandwidth sehingga semua client mendapatkan jatah bandwidth yang seimbang. Pada konfigurasi kali ini diperlukan perlengkapan seperti router mikrotik, Winbox, Laptop/PC dan Koneksi internet.



**Gambar 2.** Konfigurasi User Profile

**Konfigurasi User**

Konfigurasi user berfungsi untuk membuat atau menghapus data user/password untuk login ke hotspot.



**Gambar 3.** Konfigurasi User

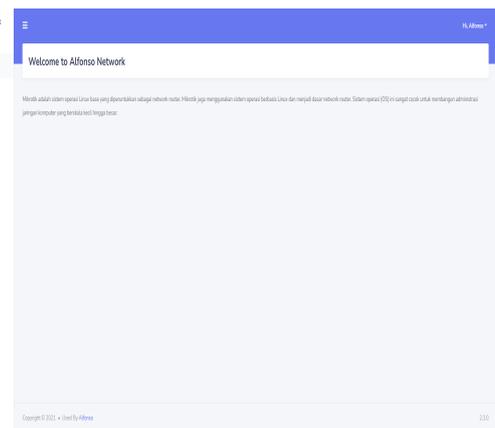
**Instalasi Squid Proxy**

Konfigurasi Proxy diperlukan sebagai Pembatas antara jaringan lokal dan jaringan internet (gateway), dengan adanya gateway ini maka sejumlah koneksi dari pengguna yang terdapat pada jaringan lokal akan terhubung ke squid, begitu juga dengan koneksi dari jaringan internet. Gateway ini sangat penting karena jaringan lokal harus dapat dilindungi dengan baik dari bahaya yang mungkin berasal dari jaringan internet. Selain sebagai gateway, masih banyak lagi fungsi dari proxy server diantaranya sebagai filtering (akses dan pengguna internet), caching, pengaturan waktu akses dan sebagainya.

**HASIL DAN PEMBAHASAN**

**Tampilan Menu Admin**

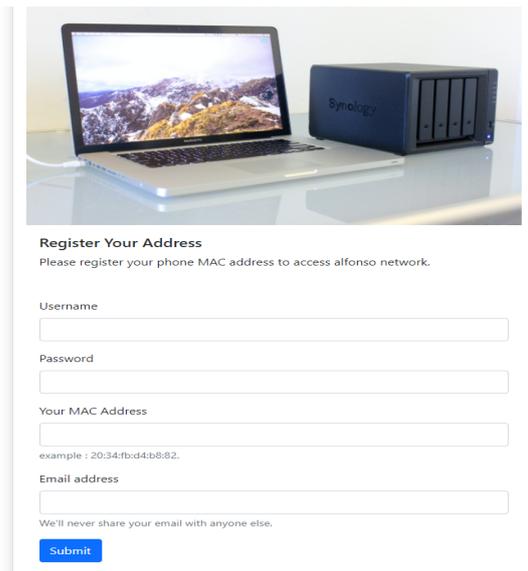
Pada tahapan ini, Admin masuk pada aplikasi winbox, memilih menu IP>Hotspot . Admin akan membuat pada user profile, yang dapat membuat management Bandwidthnya, setelah itu memilih menu user pada Hotspot untuk dapat membuat user dan mengisi data client yang sudah mendaftar username password, Mac Address, Email, Lalu memilih profile yang sudah dibuat tadi. Tampilan admin ditunjukkan pada gambar 4 berikut:



**Gambar 4.** Tampilan Admin

**Tampilan Pendaftaran Client**

Pada tampilan client akan mempersiapkan username, Password, Mac Address, Email. Pada Mac Address untuk memulai pendaftaran pada client, supaya dapat login. Proses pendaftaran pada client ditunjukkan pada gambar 5 berikut:

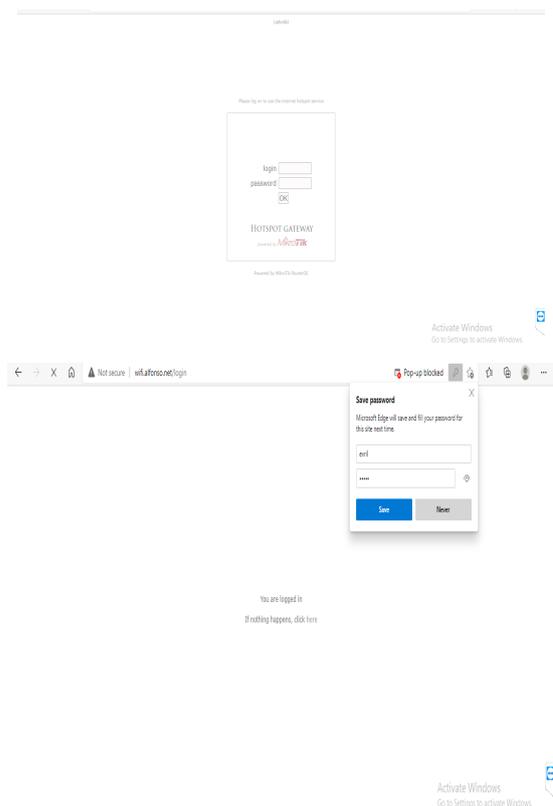


Gambar 5. Pendaftaran Pada Client

### Pengujian Mikrotik

#### Login Hotspot

Pada Login Hotspot, login dengan username dan password yang telah dibuat pada langkah sebelumnya. Jika berhasil login maka akan membuka halaman web yang diminta dan membuka popup halaman status Hotspot.



Gambar 6. Login Hotspot

Pada Konfigurasi Administrator di Mikrotik maka admin terlebih dahulu masuk pada aplikasi winbox, lalu memilih menu IP>Hostpot, selanjutnya admin akan membuat user profile lalu membuat management bandwidthnya setelah itu, Lalu pilih lagi menu user pada Hostpot untuk membuat user dan mengisi data client yang sudah mendaftar username, password, Mac Address, Email. Langkah selanjutnya pilih profile yang telah dibuat tadi lalu pilih oke.

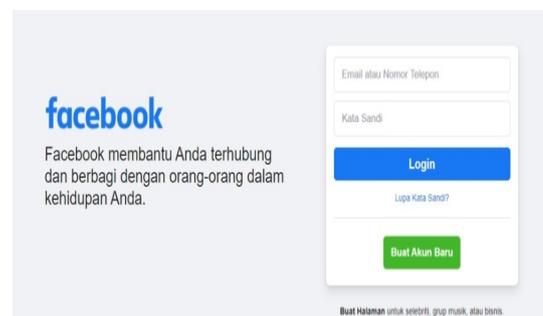
Pada komputer Client akan mempersiapkan username, password, mac address, email. Pada Mac Address dapat dilihat dengan aplikasi command Prompt pada windows dan mencantumkan IP Config/all, Mac Address juga dapat dilihat dengan kata Physical pada CMD

### Pengujian Proxy Server

#### Pengujian Filtering Content

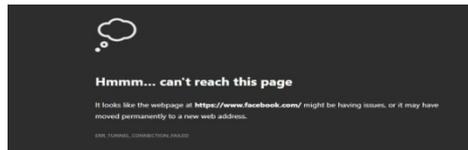
Pengujian filtering content dilakukan pada komputer client, pengujian ini dilakukan untuk menguji apakah content yang telah di filter oleh proxy server dapat di akses oleh client atau tidak dan apakah pengalokasian filtering ini telah berjalan sesuai dengan perancangan sebelumnya. Filtering ini dapat dibagi menjadi 2 bagian, yaitu:

1. Content situs jejaring sosial berdasarkan waktu Pengujian ini dapat dilakukan dengan mengakses situs yang dapat di filter seperti [www.facebook.com](http://www.facebook.com), permintaan situs akan diterima oleh proxy karena waktu pemaksaan tergolong pada jam 12:15:00



Gambar 7. Dapat Mengakses Facebook Pada Jam 12:00-15:00

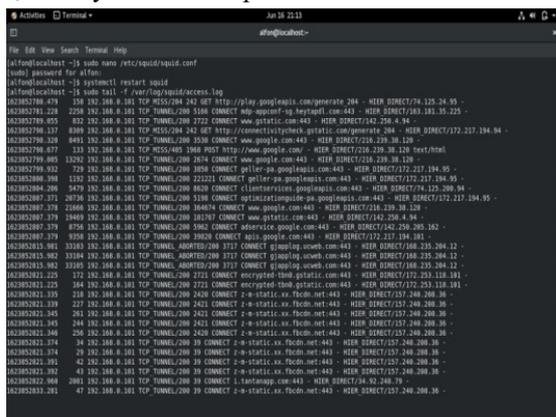
2. Pada Access Control List jam blokir situs tidak dapat mengakses [www.facebook.com](http://www.facebook.com) karena sesuai dengan waktu jam kerja yang berlaku, maka permintaan situs tersebut akan di blokir atau ditolak oleh proxy.



Gambar 8. Situs Terblock pada Jam 08:00 - 11:55

### Hasil Uji Monitoring

Pada hasil pengujian MAC Address yang didaftarkan pada squid akan tampil seperti pada sewaktu user dapat menggunakan internet. Sehingga apa yang diakses oleh client di web browser akan tampil secara keseluruhan. contohnya pada pengujian dihalaman media social [www.facebook.com](http://www.facebook.com) berikut ini, hasilnya akan ditampilkan secara keseluruhan.



Gambar 9. Tampilan Memonitoring User

### KESIMPULAN

Dari hasil penelitian yang telah dilakukan disertai dengan proses pengujian dapat ditarik kesimpulan bahwa dengan implementasi monitoring akses jaringan menggunakan squid proxy dengan menggunakan metode implementasi standard access control list mampu meminimalisir kebocoran penggunaan bandwidth internet dan membatasi pengguna sehingga akses internet lebih terjaga. Selain itu dengan di terapkanya Access Control List pada Squid Proxy penggunaan sumber daya internet lebih efektif dan lebih menghemat biaya pemeliharaan.

### DAFTAR PUSTAKA

Direktorat Operasi Keamanan Siber. (2014, April 2). 500 Juta Data Pengguna Bocor di Internet. <https://idsirtii.or.id/>.

Hafizh, M. (2011). *Load balancing dengan metode Per Connection Classifier (PCC) menggunakan proxy server sebagai caching*. UIN Syarif Hidayatullah Jakarta.

Hafizhan, M., Wahyuddin, M. I., & Komalasari, R. T. (2020). Implementasi Packet Filtering Menggunakan Metode Extended Access Control List (ACL) Pada Protokol EIGRP. *Jurnal Media Informatika Budidarma*, 4(1), 185.

<https://doi.org/10.30865/mib.v4i1.1926>

Khasanah, F. N. (2017). Squid Proxy Server untuk Peningkatan Performa Akses Internet Pada Ubuntu Server 10.10. *Bina Insani ICT Journal*, 4(1), 1–8.

Kurniawan, E. (2012). *Otentifikasi Jaringan Wireless dan Wired menggunakan Squid Proxy dan LDAP Pada Sistem Operasi Linux Ubuntu*. Universitas Muhammadiyah Surakarta.

Laksono, A. T., & Nasution, M. A. H. (2020). Implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X. *Jurnal Sistem Komputer Dan Informatika (JSON)*, 1(2), 83–88. <https://doi.org/10.30865/json.v1i2.1920>

Maulana, W. A., & Erlansyah, D. (2017). Analisis dan Management Bandwidth menggunakan metode Access Control List (Studi Kasus : PDAM Tirta Musi Palembang). *Jurnal Ilmiah Matrik*, 19(2), 1–8.

Permana, F. A. (2015, May 12). Indonesia Urutan Kedua Terbesar Negara Asal “Cyber Crime” di Dunia. *Kompas.Com*.

Purwanto, P., Kusriani, K., & Huizen, R. R. (2017). MANAJEMEN JARINGAN INTERNET SEKOLAH MENGGUNAKAN ROUTER MIKROTIK DAN PROXY SERVER. *Respati*, 11(32), 1–35. <https://doi.org/10.35842/jtir.v11i32.117>

Ritonga, M. U., Saragih, N. F., & Gea, A. (2020). PERANCANGAN APLIKASI CAPTURE TRAFFIC NETWORK TCP/IP MENGGUNAKAN NODE.JS BERBASIS WEB. *METHODIKA: Jurnal Teknik Informatika Dan Sistem Informasi*, 6(2), 14–18. <https://doi.org/10.46880/mtk.v6i2.238>