JUTIK : Jurnal Teknologi Informasi dan Komputer
Oktober-2025, Vol. 11, No.2, Hal.164-174
ISSN(P): 2442-241X; ISSN(E): 2528-5211

SIMULASI DAN IMPLEMENTASI *FIREWALL* BERBASIS *SQUID* UNTUK KEAMANAN INTERNET

Iwan Agi Berutu[1*], Khildan Rifail Azis[2], Yunita Rahmi[3], Dedy Kiswanto[4]
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[1]
Email*: iwanberutu962@gmail.com
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[2]
Email : rifadj20@gmail.com
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[3]
yunitarahmidaulay310504@gmail.com
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[4]
dedykiswanto@unimed.ac.id

ABSTRAK

Keamanan jaringan merupakan aspek penting dalam sistem informasi, terutama pada jaringan internal instansi atau organisasi. Penelitian ini bertujuan untuk mengembangkan sistem *firewall* berbasis Squid sebagai solusi keamanan jaringan yang efektif untuk mengontrol dan memfilter akses *internet*. Metode yang digunakan adalah pengembangan sistem berbasis *open source*, dengan memanfaatkan perangkat lunak Debian Linux dan Squid Proxy. Proses instalasi dan konfigurasi dilakukan untuk mengatur pembatasan akses berdasarkan protokol HTTP/HTTPS, alamat IP, dan waktu penggunaan. Hasil implementasi menunjukkan bahwa sistem *firewall* yang dibangun mampu memblokir situs yang tidak diinginkan, mengatur waktu akses, serta mencatat aktivitas pengguna melalui *log* sistem. Sistem ini juga memberikan kemudahan bagi administrator dalam memantau dan mengelola lalu lintas jaringan secara efisien. Dengan pendekatan ini, diharapkan instansi atau organisasi dapat meningkatkan keamanan jaringan internal tanpa biaya lisensi yang tinggi. Penelitian ini memberikan kontribusi dalam pemanfaatan teknologi *open source* untuk kebutuhan keamanan jaringan secara mandiri dan terjangkau.
Kata kunci: Ubuntu, *firewall,* jaringan, *proxy*, Squid

ABSTRACT

Network security is a crucial aspect of information systems, especially in the internal networks of institutions or organizations. This study aims to develop a Squid-based firewall system as an effective network security solution to control and filter internet access. The method used involves open-source system development by utilizing Debian Linux and Squid Proxy software. Installation and configuration processes were conducted to manage access restrictions based on HTTP/HTTPS protocols, IP addresses, and usage time. The implementation results show that the developed firewall system is capable of blocking unwanted websites, regulating access times, and recording user activities through system logs. This system also offers ease for administrators in monitoring and managing network traffic efficiently. With this approach, institutions or organizations are expected to enhance their internal network security without incurring high licensing costs. This research contributes to the utilization of open-source technology for independently and affordably addressing network security needs.
Keywords: Ubuntu, *firewall,* network, *proxy,* Squid

Submitted: 11 April 2025
Accepted: 15 September 2025
Published: 10 Oktober 2025

1. PENDAHULUAN

Pada saat ini perkembangan teknologi sangatlah pesat apalagi dengan didukungnya fasilitas internet yang sangat mumpuni. Namun disamping itu semua pasti selalu ada kerugian yang didapat oleh pengguna internet tersebut. Seperti serangan dari pihak-pihak yang tidak bertanggung jawab atau sering disebut dengan *hacker*. Oleh karena itu seorang administrator jaringan harus memastikan bahwa sistem jaringan komputer sebuah perusahaan harus aman dari serangan *hacker* [1].

Dalam era digital modern, kebutuhan akan jaringan internet yang cepat dan aman menjadi aspek penting dalam mendukung berbagai sektor, baik pendidikan, pemerintahan, hingga bisnis. Meningkatnya penggunaan internet telah membuka celah bagi berbagai ancaman seperti *malware*, pencurian data, dan akses terhadap konten yang tidak sesuai. Oleh karena itu, pengamanan jaringan menjadi salah satu perhatian utama dalam pengelolaan infrastruktur teknologi informasi [2] .

Internet adalah salah satu dampak modernisasi dalam bidang teknologi informasi. Berdasarkan situs datareportal.com terungkap bahwa pengguna Internet di seluruh dunia pada tahun 2024 telah mencapai angka 5,35 miliar pengguna, meningkat 1,8% dari tahun lalu, dengan 97 juta pengguna baru yang online untuk pertama kalinya selama tahun 2023 [3].

Salah satu solusi pengamanan jaringan yang banyak diterapkan adalah sistem *firewall*, yakni mekanisme pengontrol lalu lintas data yang masuk dan keluar dari jaringan. Di antara berbagai jenis *firewall*, penggunaan *Squid Proxy Server* menjadi opsi menarik karena bersifat *open-source*, fleksibel, dan memiliki fitur *caching* serta *filtering* yang bermanfaat dalam mengatur akses jaringan secara efisien [4]. Squid mampu mengatur trafik jaringan berdasarkan kebijakan tertentu, termasuk membatasi akses ke situs-situs yang tidak mendukung produktivitas atau yang dapat membahayakan sistem jaringan [5].

Implementasi *Squid Proxy Server* dalam berbagai lingkungan telah menunjukkan hasil yang positif. Misalnya, penerapan di lembaga pendidikan seperti SMK Negeri 3 Seluma mampu meningkatkan keamanan serta efisiensi jaringan dengan melakukan pembatasan akses terhadap media sosial dan situs hiburan lainnya yang tidak relevan dengan kegiatan belajar-mengajar. Studi lain juga menyebutkan bahwa *Squid* dapat menjadi solusi efektif dalam mengontrol penggunaan *bandwidth* serta memantau aktivitas pengguna dalam jaringan [6].

Namun, penggunaan *Squid* tidak lepas dari kelebihan dan kekurangan. Dari sisi keunggulan, *Squid* memungkinkan administrator untuk mengontrol akses pengguna berdasarkan IP, MAC address, dan waktu akses. Fitur *caching*-nya dapat mengurangi penggunaan *bandwidth* dan mempercepat akses ke situs yang sering dikunjungi. Selain itu, *Squid* juga mencatat *log* aktivitas pengguna, yang mempermudah proses pemantauan jaringan. *Squid* juga dapat diintegrasikan dengan sistem operasi berbasis Linux yang ringan dan stabil, menjadikannya pilihan hemat biaya [7].

Jaringan komputer tidak dapat beroperasi tanpa keamanan jaringan. Jika kerentanan jaringan komputer tidak ditambal, kerugian dapat diakibatkan oleh hilangnya data atau file, kerusakan sistem *server*, layanan pengguna di bawah standar, atau bahkan hilangnya aset institusional yang tak ternilai harganya. Karena bahaya penyerangan yang semakin canggih dan bervariasi, keamanan jaringan menjadi masalah yang sangat penting untuk diperhatikan. Ini terutama benar ketika jaringan lokal terhubung ke internet. Ancaman yang tidak bisa dihindari antara lain *Distributed Denial of Service (DDoS),* serangan *hacker*, virus, dan *trojan* [8].

Telegram bot adalah akun khusus yang tidak memerlukan sebuah nomor telepon karena sudah disiapkan oleh pihak telegram itu sendiri. Pesan, perintah, dan permintaan yang dikirim oleh pengguna diteruskan keperangkat lunak yang berjalan di *server* pemilik *telegram bot*. *Server* perantara telegram menangani semua enkripsi dan komunikasi dengan API telegram. Pengguna dapat berkomunikasi dengan *server* ini melalui antarmuka HTTPS sederhana yang menawarkan versi sederhana dari API Telegram[9].

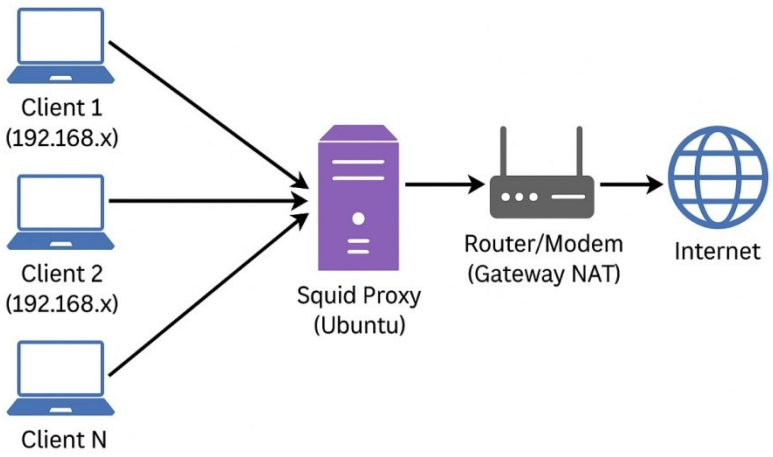
Keamanan jaringan komputer sangat penting untuk mengontrol akses jaringan dan mencegah penggunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikendalikan oleh administrator jaringan Dari sudut pandang keamanan, lima poin didefinisikan. Artinya, kerahasiaan, informasi (data) yang diperlukan hanya dapat diakses oleh pihak yang berwenang, integritas, informasi yang diperlukan hanya dapat diubah oleh pihak yang berwenang, ketersediaan, diperlukan informasi yang tersedia Peserta memiliki kewenangan sesuai kebutuhan, otentikasi, identifikasi yang benar pengirim informasi, jaminan bahwa ID yang diperoleh tidak dipalsukan, non-penyangkalan, pengirim informasi Menerima pesan, meminta penerima juga tidak dapat menolak untuk mengirim [10].

Melihat tantangan dan potensi yang ada, penelitian ini berfokus pada pengembangan sistem *firewall* berbasis *Squid* untuk meningkatkan keamanan jaringan, terutama dalam membatasi akses *internet* yang tidak sesuai dengan kebijakan institusi. Sistem ini diharapkan dapat memperkuat pengelolaan jaringan internet dengan pendekatan yang efisien, terukur, dan mudah diimplementasikan. Tujuan utama dari proyek ini adalah untuk menguji efektivitas *Squid* dalam mengontrol akses internet dan meningkatkan keamanan jaringan dengan membatasi akses ke situs tertentu. Dengan adanya sistem ini, diharapkan dapat memberikan solusi bagi administrator jaringan dalam mengelola dan mengamankan konektivitas pengguna secara lebih optimal.

2. METODE

Pada pengerjaan *proxy* ini telah dilakukan dalam beberapa tahap proses pengerjaan, tahapan-tahapan nya tergambarkan pada *flowchart* di bawah ini.

Gambar 1. *Flowchart* metode penelitian



Gambar 2. Topologi jaringan

Instalasi VirtualBox

Sebagai langkah awal, dilakukan instalasi VirtualBox pada sistem host. VirtualBox dipilih karena merupakan perangkat lunak *virtualisasi* yang memungkinkan pembuatan dan pengelolaan mesin virtual dengan fleksibilitas tinggi. Dengan menggunakan VirtualBox, dapat dibuat lingkungan uji coba yang aman dan terkendali tanpa mempengaruhi sistem utama.

Instalasi dan Konfigurasi Ubuntu

Setelah VirtualBox berhasil diinstal, tahap berikutnya adalah pembuatan mesin virtual dengan spesifikasi yang sesuai untuk menjalankan layanan *proxy* berbasis Squid. Sistem operasi yang dipilih adalah Ubuntu karena stabilitas dan dukungan komunitas yang luas. Instalasi Ubuntu dilakukan dengan konfigurasi awal yang mencakup pengaturan jaringan, pembaruan sistem, serta pemasangan alat bantu yang diperlukan untuk mempermudah proses pengelolaan *server*.

Pembuatan Mesin Virtual

Mesin virtual yang dibuat telah dikonfigurasi dengan alokasi sumber daya yang cukup untuk menjalankan Squid secara optimal. Parameter seperti jumlah CPU, RAM, dan ruang penyimpanan telah disesuaikan agar mampu menangani lalu lintas jaringan dalam skala kecil hingga menengah. Selain itu, pengaturan jaringan telah dikonfigurasi agar mesin virtual dapat terhubung dengan jaringan lokal dan menjalankan fungsinya sebagai *firewall.*

Instalasi Squid

Squid telah berhasil diinstal pada Ubuntu dalam mesin virtual. Instalasi dilakukan dengan menggunakan manajer paket bawaan Ubuntu dan dikonfigurasi agar dapat berfungsi sebagai *proxy server*. Beberapa parameter utama telah disesuaikan, seperti pengaturan *cache*, akses kontrol, serta mekanisme pemblokiran berdasarkan daftar *domain* yang telah ditentukan.

Pengujian Pemblokiran Situs

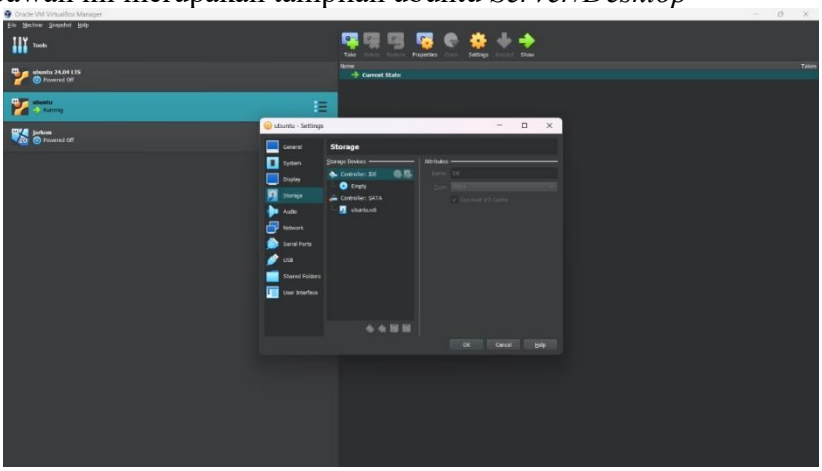
Sebagai bagian dari pengujian, Squid telah dikonfigurasi untuk memblokir akses ke beberapa situs tertentu, seperti TikTok.com dan Netflix.com. Pengujian dilakukan dengan mencoba mengakses situs-situs tersebut dari klien yang terhubung ke jaringan yang dikelola oleh Squid. Hasil pengujian menunjukkan bahwa akses ke situs yang telah ditentukan berhasil diblokir sesuai dengan aturan yang telah diterapkan. Hal ini menegaskan bahwa sistem bekerja dengan baik dalam mengontrol akses pengguna terhadap konten di *internet.*

3. HASIL DAN PEMBAHASAN

Proxy server berfungsi sebagai perantara antara klien dan *internet.* Salah satu software *proxy* yang populer di sistem operasi Linux, khususnya Ubuntu, adalah Squid. Dalam proyek ini, Squid digunakan untuk mengatur akses *internet*, termasuk memblokir situs tertentu. Adapun Langkah-Langkah Konfigurasi *Proxy Server* di Ubuntu adalah sebagai berikut :

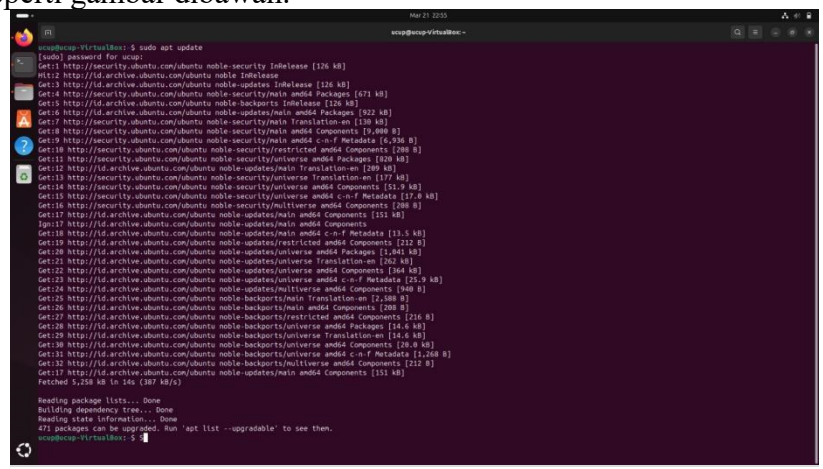
Persiapan Sistem

1. Sistem operasi: Ubuntu Server/Desktop (20.04 LTS atau 22.04 LTS)
   Gambar dibawah ini merupakan tampilan ubuntu *Server*/*Desktop*



Gambar 3. Ubuntu *server*/*desktop*

2. *Update system*
   Selanjutnya perintah: sudo apt update && sudo apt upgrade, maka akan muncul tampilan seperti gambar dibawah.



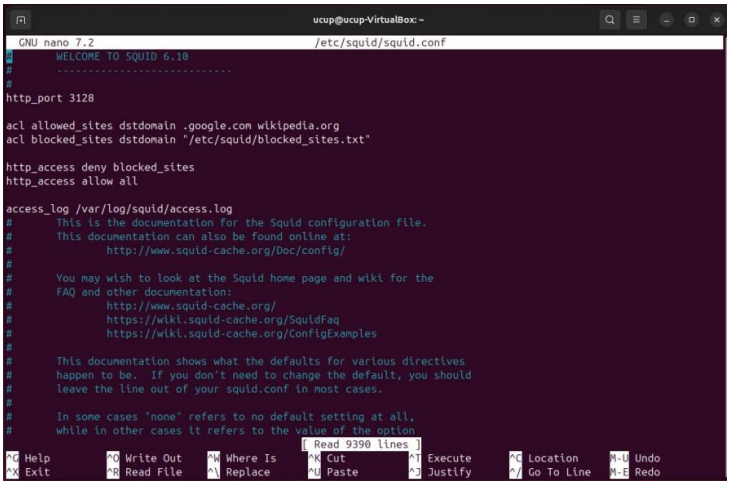
Gambar 4. Tampilan sudo apt update

Instalasi Squid

Dengan cara perintah: sudo apt install squid, selanjutnya edit file konfigurasi utama squid yaitu dengan perintah "sudo nano/etc/squid/squid.conf" dan juga tambahkan konfigurasi berikut:

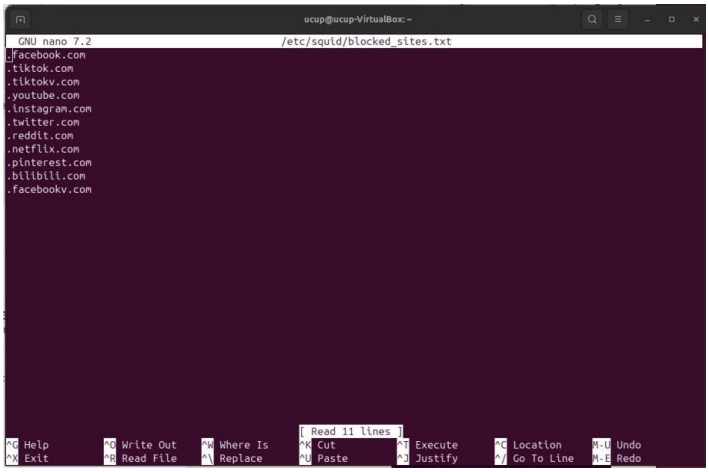
```
http_port 3128

acl allowed_sites dstdomain .google.com wikipedia.org
acl blocked_sites dstdomain "/etc/squid/blocked_sites.txt"

http_access deny blocked_sites
http_access allow all

access_log /var/log/squid/access.log
```

Maka akan muncul seperti gambar berikut



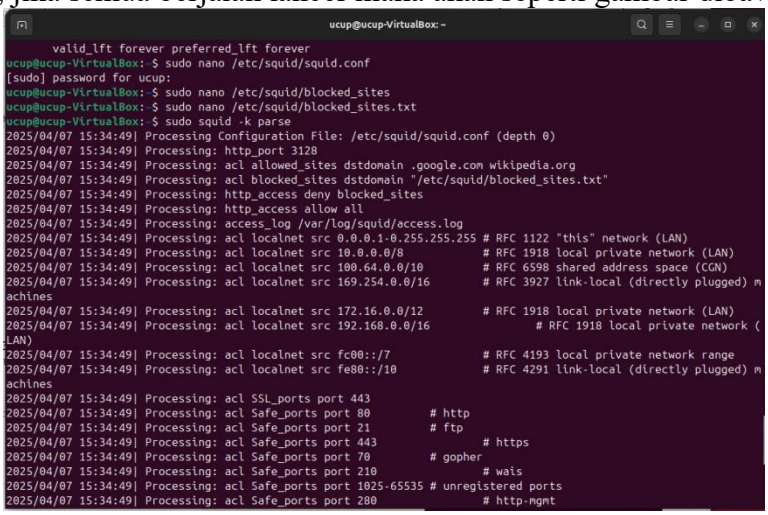
Gambar 5. Tampilan konfigurasi squid

Selanjutnya buat file yang berisi daftar situs yang ingin di blokir dengan perintah sudo nano /etc/squid/blocked_sites.txt. Contoh isi yang igin di blokir bisa berupa tiktok.com, facebook.com, Instagram.com dll. Dapat dilihat pada Gambar 6.



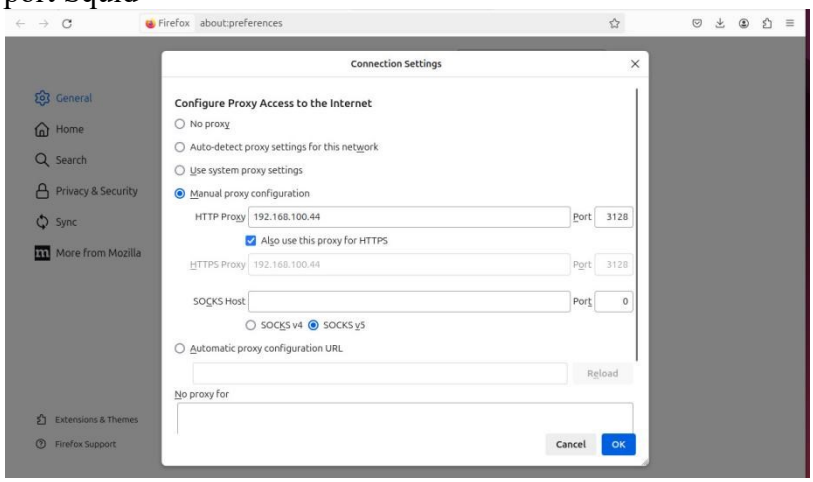
Gambar 6. Tampilan *file* blokir situs

Pastikan tidak terjadi kesalahan saat konfigurasi, cek konfigurasi dengan perintah sudo squid -k parse, jika semua berjalan lancer maka akan seperti gambar dibawah ini



Gambar 7. Tampilan konfigurasi berjalan lancer

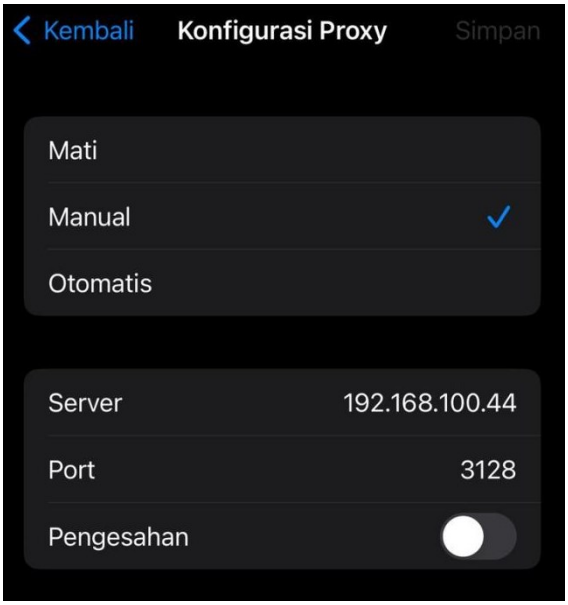
Seperti itulah proses kerja dari Konfigurasi *Proxy Server* di Ubuntu, jika ingin merestart squid bisa menggunkan konfiguarasi sudo systemctl restart squid. *Proxy* bisa disetting di laptop windows ataupun MacOS, melalui IP address Ubuntu *server* dengan Port: 3128 atau di *browser* dengan cara buka pengaturan jaringan, klik *proxy* dan isi alamat IP & port Squid



Gambar 8. Settingan di browser

Nah pada gambar diatas merupakan setingan *proxy* jika anda menyeting melalui *browser* atau juga bisa melalui *handphone* dengan cara:

1. Sambungkan ke jaringan yang sama dengan *server*/ ubuntunya, klik pengaturan wifi.
2. Klik icon yang huruf I di ujung kanan wifi yang di hubungkan
3. Scrol ke bawah sampai ketemu " konfigurasi *proxy*"
4. Lalu pilih manual dan masukkan ip *server proxy* dan port nya server: 192.168.100.44 dan port: 3128
5. lalu klik simpan



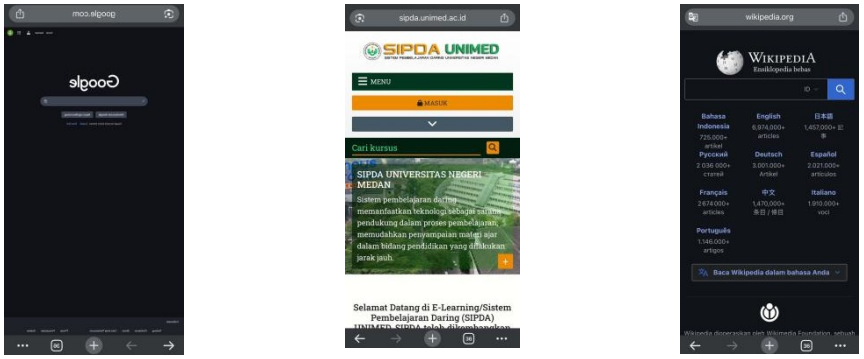
Gambar 9. Tampilan setting di *handphone*

Jika anda melakukan di hanphone maka tampilan akan seperti gambar diatas.

Uji coba dari *proxy* seperti akases situs yang diperbolehkan seperti google.com atau Wikipedia dan sipda unimed. Jika uji coba bisa maka akan muncul tampilan seperti gambar di bawah

Google.com Sipda unimed Wikipedia.org

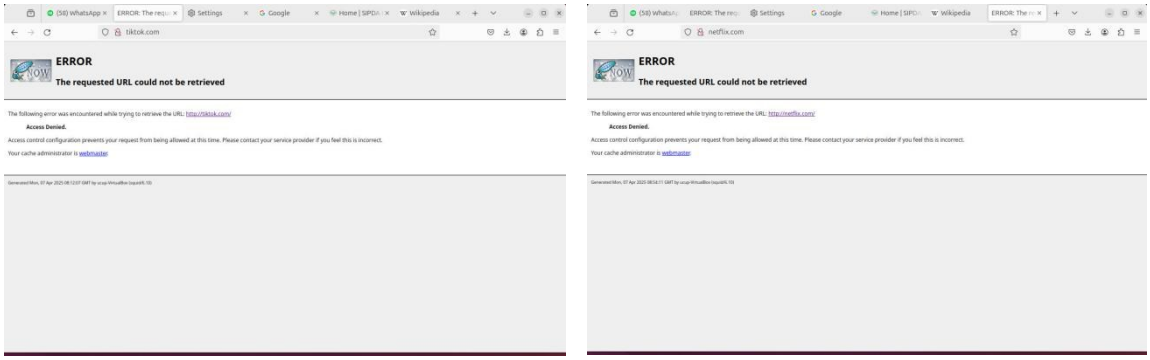
Gambar 10. Tampilan pada laptop



Google.com Sipda unimed Wikipedia.org

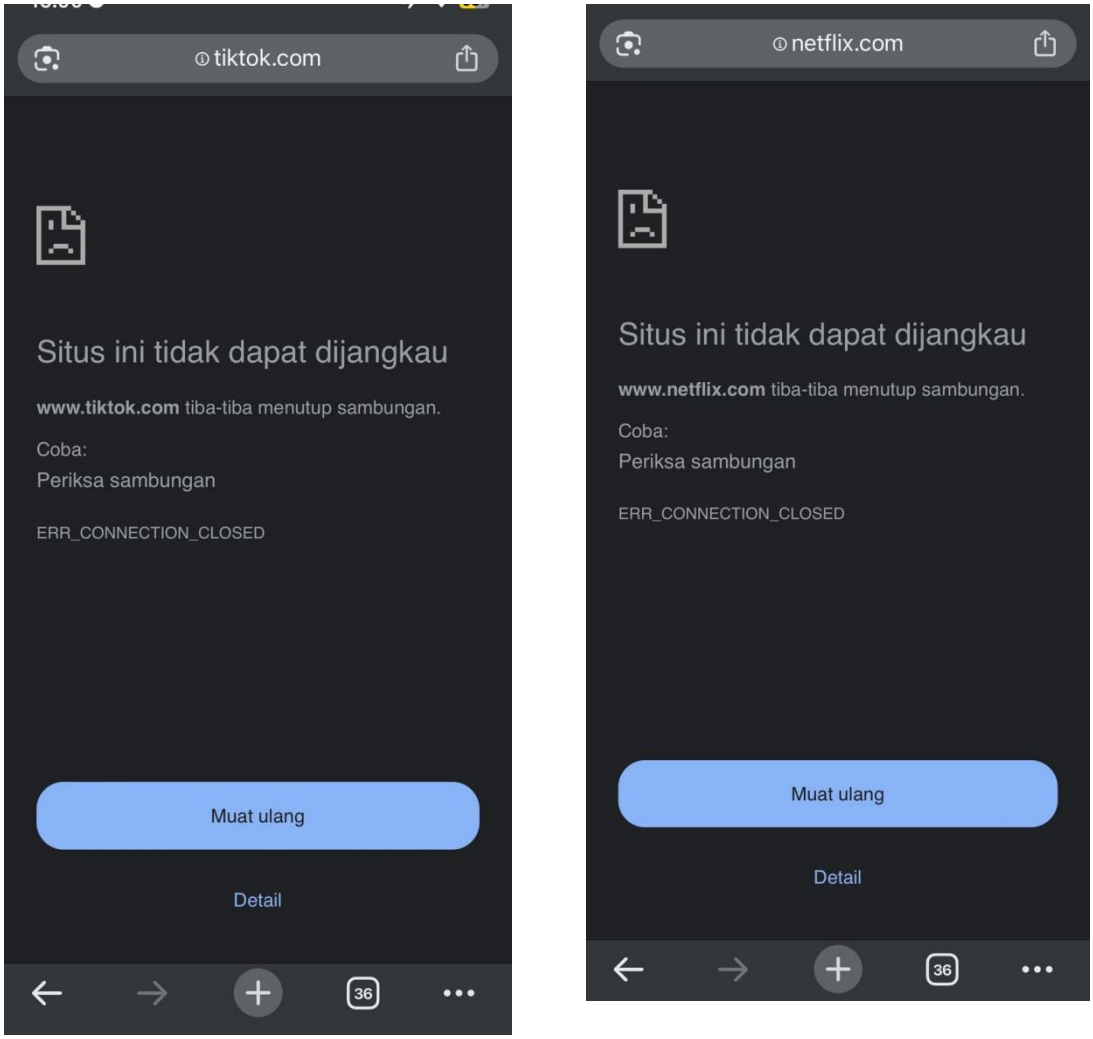
Gambar 11. Tampilan pada HP

Untuk akses yang di blokir maka akan muncul *error* seperti pada Gambar 12 dan 13 dibawah ini.



Tiktok.com Netflix.com

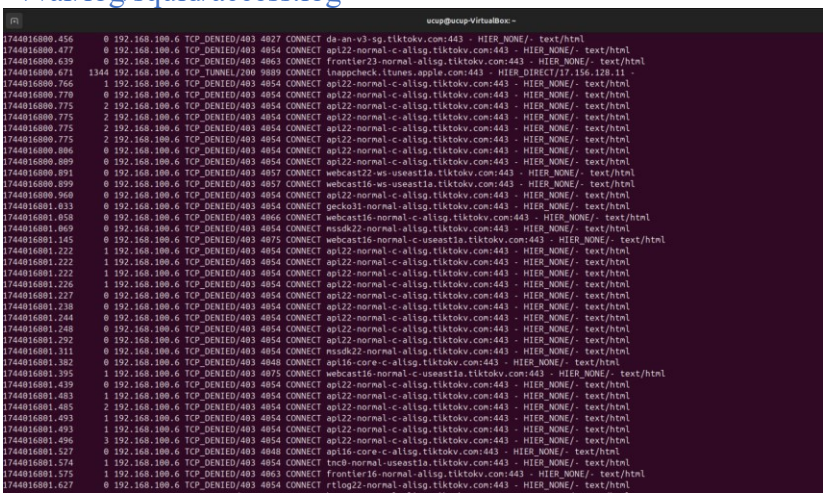
Gambar 12. Tampilan di laptop



Tiktok.com Netflix.com

Gambar 13. Tampilan di HP

Untuk melihat Log Akses bisa menggunakan konfigurasi dengan perintah :
sudo tail -f /var/log/squid/access.log



Gambar 14. Tampilan *traffic* jaringan

4. KESIMPULAN DAN SARAN

Dengan menggunakan Ubuntu dan Squid, kita dapat membuat *proxy server* yang bisa membatasi akses ke situs tertentu. Hal ini bermanfaat untuk lingkungan sekolah, kantor, atau warnet.

DAFTAR PUSTAKA

[1] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *Aiti*, vol. 17, no. 2, pp. 143–158, 2021, doi: 10.24246/aiti.v17i2.143-158.

[2] D. A. Artika, B. D. Febrianti, S. P. Syaifullah, D. Kiswanto, I. Komputer, and U. N. Medan, "Mengimplementasikan Proxy Server (Squid Server)," *JATI (J. Mahasiswa Teknik Informatika),*vol. 8, no. 6, pp. 12512–12520, 2024.

[3] S. Dwiyatno, E. Rakhmat, S. Sulistiyono, and M. R. Mahruzzaman, "Penerapan Internet Sehat Sebagai Internet Service Provider Menggunakan Network Monitoring System Zabbix Dan Squid Proxy," *J. Innov. Futur. Technol.*, vol. 3, no. 2, pp. 25–40, 2021, doi: 10.47080/iftech.v3i2.1532.

[4] M. 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: 10.32528/justindo.v9i1.981.

[5] I. Saputra, T. U. Kalsum, and H. Alamsyah, "The Implementation Of Network Management And Security Using Mikrotik And Proxy Server At SMK N 3 Seluma," *J. Media Comput. Sci.*, vol. 3, no. 1, pp. 17–32, 2024, doi: 10.37676/jmcs.v3i1.5422.

[6] A. Susanto, "Pengaturan Keamanan Squid Proxy Pada Jaringan Lokal Dan Internet Menggunkan Openldap," *J. Teknol. Pint.*, vol. 2, no. 3, pp. 1–13, 2022, [Online]. Available: http://teknologipintar.org/index.php/teknologipintar/article/view/121

[7] N. A. Santoso, K. B. Affandi, and R. D. Kurniawan, "Implementasi Keamanan Jaringan Menggunakan Port Knocking," *J. Janitra Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 90–95, 2022, doi: 10.25008/janitra.v2i2.156.

[8] A. Bustami and S. Bahri, "Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi : Systematic Review," *Unistek*, vol. 7, no. 2, pp. 59–70, 2020, doi: 10.33592/unistek.v7i2.645.

[9] Farhan, Dwi,Rifda, "IMPLEMENTASI BOT TELEGRAM UNTUK MONITORING MIKROTIK PADA PLANETS NETWORK SOLUTION" *Jurnal Teknologi Informasi dan Komputer, Volume 9, Nomor 6, Oktober 2023*

[10] Gea, A., Purba, M. J., Putra, A. A., Jamaluddin, J., & Siringoringo, R. (2022). Implementasi Metode Access Control List Untuk Memonitoring Akses Jaringan Menggunakan Squid Proxy. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, *6*(1), 79-84.