IMPLEMENTASI SQUID PROXY SEBAGAI FIREWALL UNTUK PENGELOLAAN KEAMANAN JARINGAN

Ahmad Denil Sitepu[1], Bob Valentino[2], Idris Putra Hatoguan[3], Dedy Kiswanto[4]
adenilsitepu@gmail.com[1], bobvalentino46@gmail.com[2], idrisputra76@gmail.com[3], dedykiswanto@unimed.ac.id[4]
Universitas Negeri Medan

ABSTRACT

Security is a very important element in a computer network. This is done in an effort to provide protection to the computer network to prevent threats from both internal and external in an effort to prevent forced (unauthorized) data retrieval. A network security system needs to be built to control access to important assets, one of which is data, so that the access rights of each computer and user need to be regulated. The Squid proxy method is one technique that can be used to regulate access from users and computers. Squid proxy can be used to regulate network access rights on each LAN (Local Area Network) port. This is very useful for blocking access from one party to another to prevent data theft from unknown or known people. From the tests carried out, it is known that the implementation of a firewall can block the network connection when there is a transfer of access rights.

Keywords: *Network Security, Firewall, Squid Proxy, Hak Akses, Web.*

PENDAHULUAN

Dalam era digital saat ini, teknologi informasi telah menjadi bagian yang tidak terpisahkan dari berbagai sektor, termasuk bisnis, pendidikan, pemerintahan, dan industri lainnya. Perkembangan teknologi juga berdampingan dengan jaringan, sehingga network engineer adalah salah satu profesi yang paling dibutuhkan saat ini [1]. Konektivitas internet yang semakin luas memberikan banyak manfaat, seperti kemudahan dalam berbagi informasi, komunikasi yang lebih efisien, serta akses yang lebih cepat terhadap berbagai layanan digital. Namun, di balik manfaat tersebut, keamanan jaringan menjadi tantangan utama yang harus dihadapi oleh organisasi dalam menjaga integritas, kerahasiaan, dan ketersediaan data mereka.[2].

Ancaman siber seperti peretasan, pencurian data, penyebaran malware, dan akses ilegal terhadap sistem informasi terus meningkat seiring dengan semakin kompleksnya teknologi yang digunakan. Keamanan jaringan merupakan salah hal yang pentig untuk dijaga dan dikelola dikarenakan keamanan jaringan yang tidak terkelola dengan baik dapat mengakibatkan kebocoran informasi rahasia, gangguan terhadap operasional sistem, hingga potensi kerugian finansial yang besar [3]. Oleh karena itu, diperlukan suatu sistem keamanan yang mampu memberikan perlindungan terhadap ancaman tersebut, sekaligus mengontrol serta mengelola aktivitas pengguna dalam jaringan. Dalam konteks keamanan jaringan, system keamanan ini sering disebut sebagi port security [4].

Salah satu terobosan dari system keamanan jaringan tadi adalah web proxy dan squid proxy. Web proxy digunakan untuk menyembunyikan IP pengguna dan juga berfungsi untuk memberikan akses kepada pengguna dalam mengakses website yang terblokir [5]. Terkait dengan web proxy, terdapat juga salah satu solusi yang bekerja sebagai perangkat lunak, yaitu Squid proxy atau sering juga disebut sebagai proxy server.Squid Proxy merupakan perangkat lunak open-source yang berfungsi sebagai server proxy dan mampu mengatur lalu lintas jaringan dengan menerapkan kebijakan keamanan tertentu. Dengan konfigurasi yang tepat, Squid Proxy dapat berperan sebagai firewall yang mampu menyaring lalu lintas jaringan, memblokir akses ke situs web tertentu, serta mencegah

ancaman siber yang berasal dari luar maupun dalam jaringan [6].

Server proxy juga dapat didefenisikan sebagai perangkat atau computer yang digunakan untuk menyediakan jaringan. Beberapa server proxy bisa berupa sekelompok aplikasi atau server yang memblokir layanan internet umum. Misalnya, proxy HTTP memotong akses web sedangkan proxy SMTP memotong akses terhadap email [7]. Terkait dengan server proxy, firewall juga memili peran dalam meningkatkan efisiensi keamanan jaringan. Proxy berfungsi sebagai perantara antara pengguna dan internet, memungkinkan penyaringan konten, penyembunyian identitas IP, serta peningkatan kecepatan akses melalui caching. Sementara itu, firewall bertugas memantau dan mengontrol lalu lintas jaringan berdasarkan aturan keamanan guna mencegah akses yang tidak sah dan ancaman dari luar [8].

Terkait dengan fungsi firewall dalam membantu meningkatkan efisiensi server proxy, kita juga perlu memahami bagaimana firewall itu sendiri bekerja. Firewall berkerja sebagai garis pertahanan pertama Anda, memantau dan mengendalikan lalu lintas antara jaringan internal dan eksternal, selain itu, firewall juga memungkinkan deteksi dan pemantauan aktivitas mencurigakan, memberikan lapisan pertahanan tambahan terhadap potensi ancaman dunia maya [9]. Salah satu fitur dari firewall adalah filtering content, yakni firewall menyaring paket berdasarkan parameter seperti IP dan port. Namun firewall biasanya hanya terdapat pada perangkat dengan skala kecil seperti PC, nah disini untuk memperuas jangkauan firewall dibutuhkan router mikrotik yang berfungsi untuk memperluas skala tersebut [10].

Pada penelitian ini lebih difokuskan dalam meneliti Squid proxy, squid Proxy memiliki berbagai keunggulan dalam mengelola keamanan jaringan, tapi jika implementasinya yang tidak tepat dapat menyebabkan kendala, seperti keterbatasan akses bagi pengguna yang sah, peningkatan latensi dalam jaringan, serta kompleksitas dalam pengelolaan konfigurasi. Oleh karena itu, diperlukan penelitian lebih lanjut untuk memahami bagaimana Squid Proxy dapat diimplementasikan secara optimal sebagai firewall guna meningkatkan keamanan jaringan tanpa mengganggu kinerja sistem yang ada.

Penelitian ini bertujuan untuk menganalisis efektivitas Squid Proxy dalam pengelolaan keamanan jaringan, mengeksplorasi strategi implementasi terbaik, serta mengidentifikasi tantangan yang mungkin dihadapi dalam penggunaannya. Dengan adanya penelitian ini, diharapkan dapat diperoleh wawasan yang lebih mendalam mengenai pemanfaatan Squid Proxy sebagai firewall serta memberikan rekomendasi bagi organisasi atau institusi yang ingin mengadopsinya sebagai bagian dari strategi keamanan jaringan mereka.

METODOLOGI

Penelitian ini dilakukan dengan pendekatan eksperimen dan deskriptif kualitatif untuk memahami bagaimana Squid Proxy dapat diterapkan sebagai firewall dalam pengelolaan keamanan jaringan. Dengan metode ini, penelitian tidak hanya berfokus pada teori, tetapi juga pada penerapan nyata Squid Proxy dalam sebuah lingkungan jaringan untuk melihat sejauh mana efektivitasnya dalam meningkatkan keamanan.

Langkah pertama dalam penelitian ini adalah melakukan studi literatur dari berbagai sumber, seperti jurnal ilmiah, buku, serta dokumentasi resmi yang membahas Squid Proxy, firewall, dan keamanan jaringan. Studi ini bertujuan untuk memahami konsep dasar, fitur utama, serta teknik konfigurasi yang dapat diterapkan dalam Squid Proxy. Selain itu, studi literatur juga membantu dalam mengetahui potensi manfaat serta kendala yang mungkin muncul selama implementasi.

Setelah pemahaman dasar diperoleh, penelitian dilanjutkan dengan perancangan dan

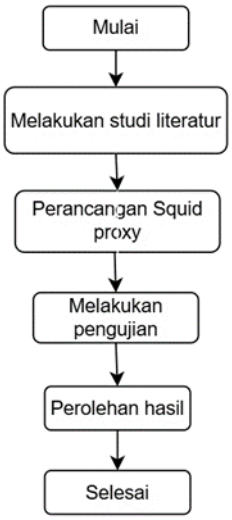
implementasi Squid Proxy dalam lingkungan jaringan yang telah disiapkan. Squid Proxy diinstal dan dikonfigurasi pada sebuah server yang bertindak sebagai pusat kontrol lalu lintas jaringan. Beberapa kebijakan keamanan diterapkan, seperti pemblokiran akses ke situs web tertentu, penyaringan konten yang tidak diinginkan, serta pembatasan hak akses bagi pengguna jaringan. Implementasi ini dilakukan dengan menyesuaikan pengaturan Squid Proxy agar sesuai dengan tujuan utama, yaitu meningkatkan keamanan jaringan tanpa mengganggu akses yang sah.

Tahap berikutnya adalah pengujian, di mana berbagai skenario diuji untuk melihat bagaimana Squid Proxy bekerja dalam kondisi nyata. Pengujian ini mencakup bagaimana sistem menyaring lalu lintas internet, memblokir akses ke situs berbahaya, serta mencatat aktivitas pengguna dalam jaringan. Selain itu, pengujian juga dilakukan untuk mengetahui apakah ada dampak negatif terhadap performa jaringan setelah implementasi Squid Proxy, seperti peningkatan latensi atau keterbatasan akses yang tidak diinginkan.

Setelah pengujian dilakukan, hasilnya dianalisis menggunakan metode deskriptif kualitatif. Data yang diperoleh dari pengujian dibandingkan dengan teori yang telah dikaji sebelumnya serta standar keamanan jaringan yang ada. Dari analisis ini, diidentifikasi sejauh mana Squid Proxy efektif dalam mengelola keamanan jaringan, apa saja kelebihan dan kekurangannya, serta bagaimana sistem ini dapat dioptimalkan agar lebih efektif.

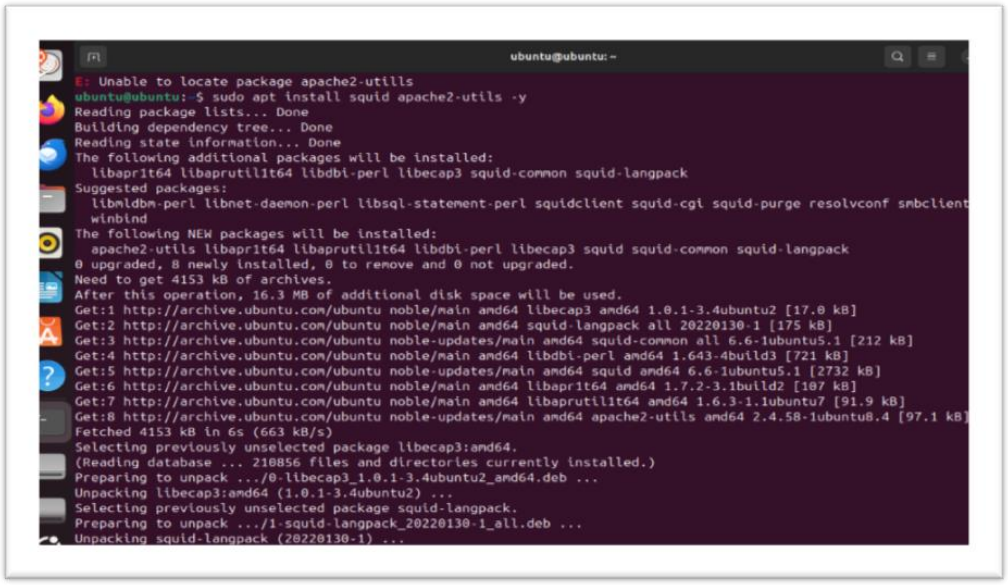
Pada tahap akhir, dilakukan evaluasi dan penyusunan kesimpulan berdasarkan seluruh rangkaian penelitian. Evaluasi ini mencakup penentuan apakah Squid Proxy dapat berfungsi dengan baik sebagai firewall, apakah dapat meningkatkan keamanan jaringan secara signifikan, serta tantangan apa saja yang muncul dalam implementasinya. Dari hasil penelitian ini, diharapkan dapat diperoleh rekomendasi yang dapat digunakan oleh organisasi atau institusi yang ingin menerapkan Squid Proxy sebagai bagian dari sistem keamanan jaringan mereka.

Dengan pendekatan ini, penelitian tidak hanya menghasilkan pemahaman teoretis, tetapi juga solusi praktis yang dapat diterapkan dalam dunia nyata untuk meningkatkan keamanan jaringan menggunakan Squid Proxy sebagai firewall. Adapun alur penelitian adalah sebagai berikut:



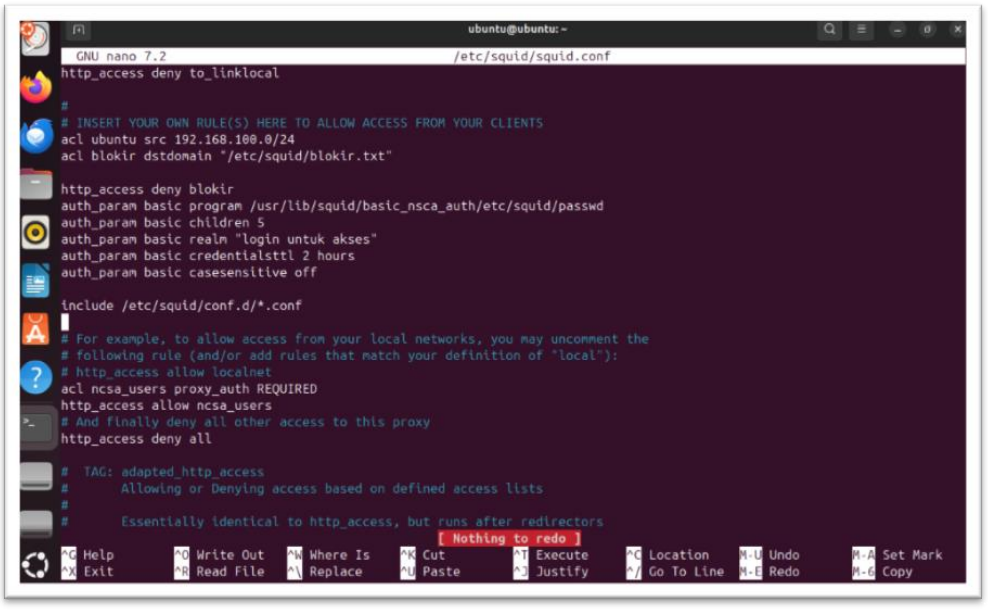
Gambar 1.

HASIL DAN PEMBAHASAN



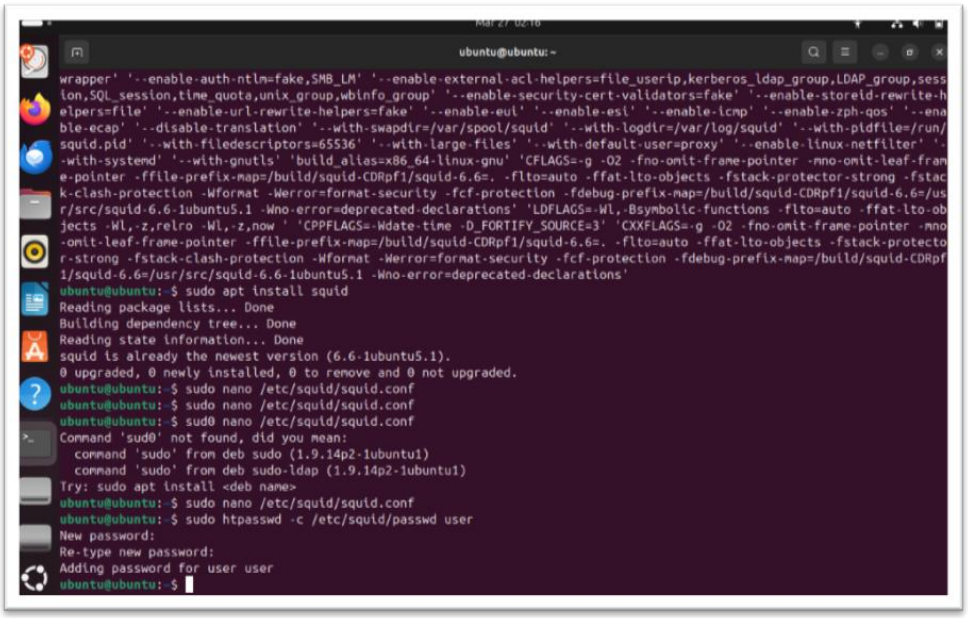
Gambar 2.

- Gambar ini menggambarkan proses instalasi perangkat lunak di ubuntu, termasuk bagaimana dependensi dikelola secara otomatis, serta bagaimana apt bekerja dalam mengunduh dan menginstal paket dari repositori resmi. Paket squid yang diinstal dapat digunakan sebagai proxy caching untuk meningkatkan efisiensi akses internet dan mengontrol lalu lintas jaringan, sementara apache2-utils menyediakan berbagai alat tambahan yang berguna bagi administrator server web apache.



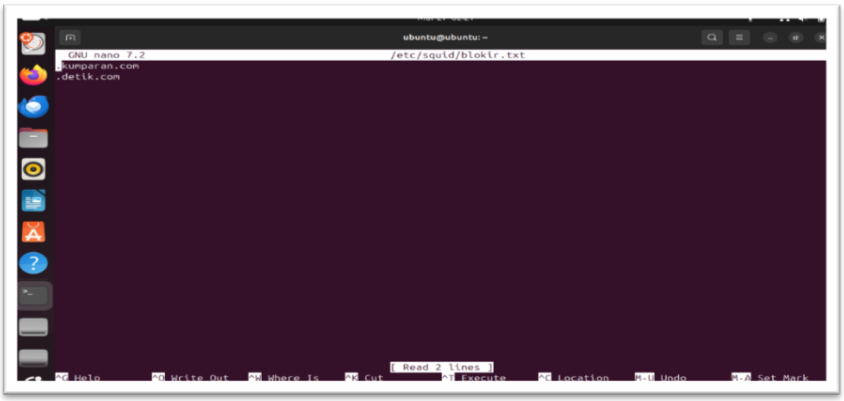
Gambar 3.

- Squid di sini dikonfigurasi untuk mengontrol akses internet dengan cukup ketat. Hanya pengguna yang sudah login yang bisa menggunakan proxy, dan ada daftar situs yang diblokir. Dengan pengaturan seperti ini, administrator jaringan bisa memastikan bahwa akses internet lebih terkontrol, tidak semua orang bisa menggunakan proxy secara bebas, dan situs-situs tertentu dapat dibatasi sesuai kebijakan yang diinginkan.



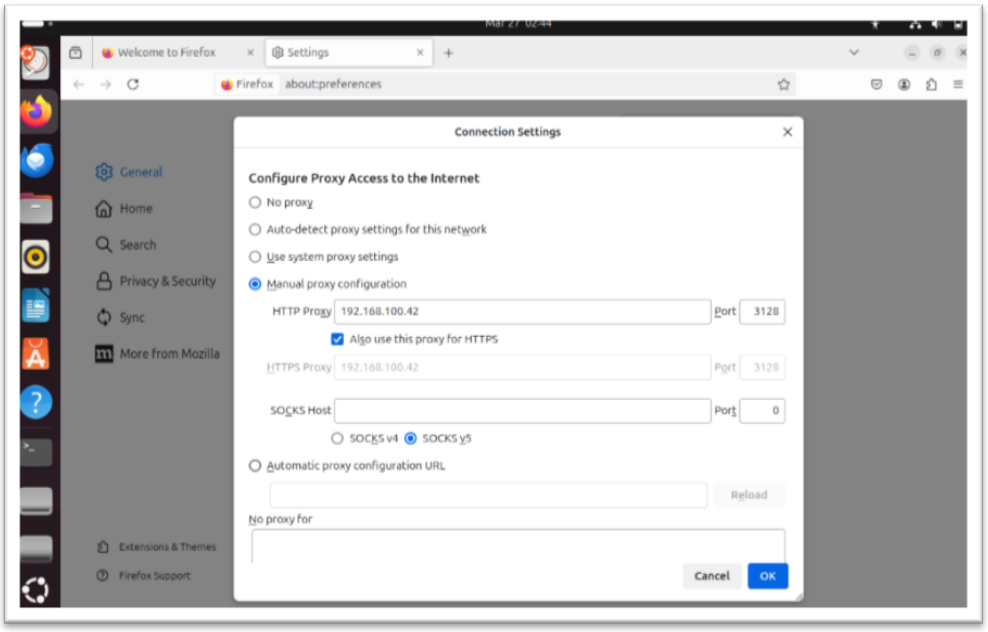
Gambar 4.

- Proses ini menunjukkan bahwa pengguna sedang menyiapkan Squid Proxy dengan sistem autentikasi username dan password. Hal ini bertujuan untuk membatasi akses ke proxy agar hanya pengguna yang memiliki kredensial yang benar yang bisa menggunakannya.



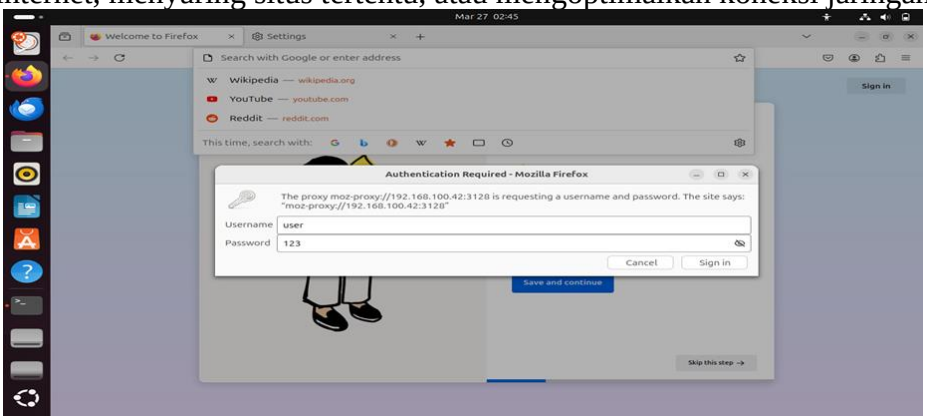
Gambar 5.

- Gambar tersebut menampilkan tampilan terminal pada sistem operasi Ubuntu, di mana pengguna sedang menggunakan editor teks GNU nano 7.2 untuk mengedit sebuah file konfigurasi bernama blokir.txt yang terletak di dalam direktori /etc/squid/. File ini digunakan untuk menyimpan daftar situs web yang akan diblokir oleh Squid Proxy.



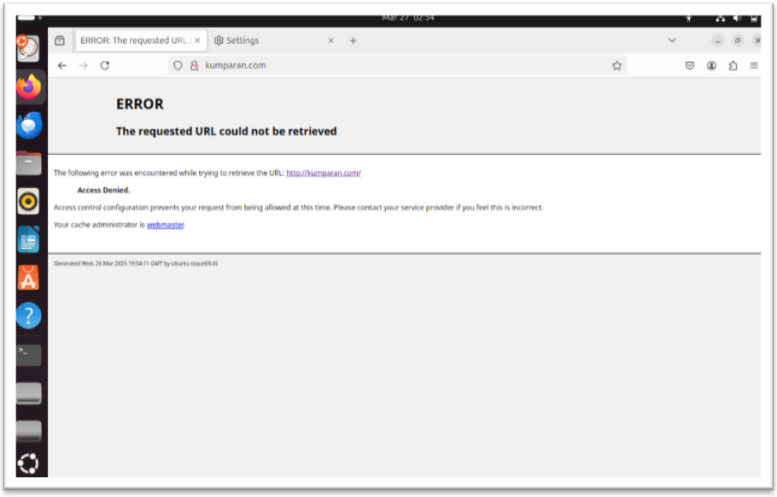
Gambar 6.

- Gambar ini menunjukkan pengaturan koneksi di Firefox pada sistem operasi Ubuntu, di mana pengguna sedang mengatur penggunaan proxy secara manual. Dalam pengaturan ini, Firefox diarahkan untuk menggunakan proxy dengan alamat 192.168.100.42 dan port 3128. Pengguna juga mencentang opsi "Also use this proxy for HTTPS", sehingga semua koneksi HTTP dan HTTPS akan melewati proxy ini. Dari pengaturan ini, terlihat bahwa Firefox akan mengarahkan semua lalu lintas internetnya melalui server proxy 192.168.100.42:3128. Ini adalah Squid Proxy, yang bisa digunakan untuk mengontrol akses internet, menyaring situs tertentu, atau mengoptimalkan koneksi jaringan.



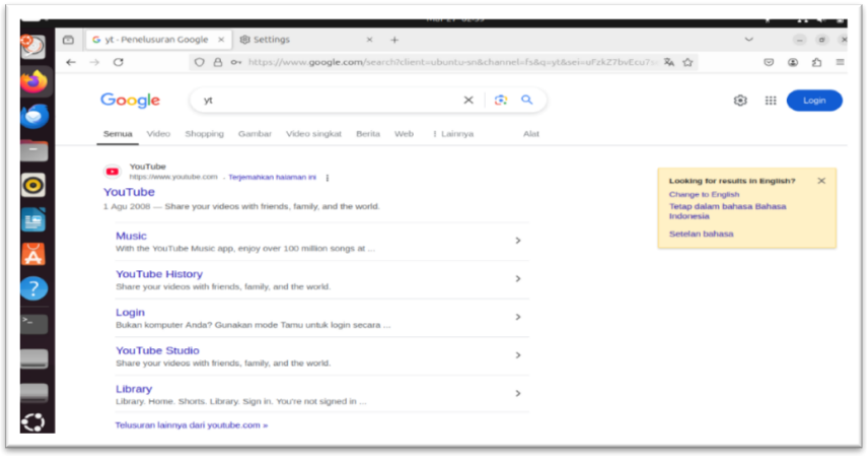
Gambar 7.

- Pada gambar ini pengguna mencoba mengakses Proxy dengan memasukkan username dan password.



Gambar 8.

- Pada gambar tersebut menunjukkan bahwa situs yang sudah di blokir tidak bisa dibuka lagi atau error. Seperti gambar di atas pengguna mencoba membuka aplikasi yang di blokir(kumparan) dan hasilnya menunjukkan error.



Gambar 9.

- Pada gambar tersebut pengguna mencoba membuka situs web yang tidak di blokir oleh firewall dan hasilnya berhasil.

KESIMPULAN

implementasi Squid Proxy sebagai firewall memberikan solusi efektif dalam mengelola keamanan jaringan. Penelitian ini mengungkapkan bahwa Squid Proxy mampu mengontrol akses internet dengan menerapkan kebijakan penyaringan yang ketat, seperti memblokir situs-situs yang dianggap tidak aman dan hanya mengizinkan akses bagi pengguna yang telah terautentikasi. Dari penerapan di lingkungan nyata, terlihat bahwa penggunaan Squid Proxy tidak hanya berfungsi sebagai alat pemantauan aktivitas pengguna, tetapi juga membantu mencegah ancaman siber seperti pencurian data dan penyebaran malware. Meskipun konfigurasi dan pengelolaan Squid Proxy memerlukan perhatian khusus untuk menghindari dampak negatif seperti peningkatan latensi atau pembatasan akses yang tidak diinginkan, hasil pengujian menunjukkan bahwa sistem ini memiliki potensi besar dalam meningkatkan keamanan jaringan. Penelitian ini juga menekankan perlunya evaluasi dan penyesuaian lebih lanjut untuk mengoptimalkan kinerja dan efektivitas firewall berbasis Squid Proxy, sehingga dapat diadaptasi sesuai dengan kebutuhan dan kebijakan keamanan

pada masing-masing organisasi.

DAFTAR PUSTAKA

D. Kiswanto, H. Syahputra, dan S. Panggabean, "Training Peningkatan Kompetensi Industri untuk Sertifikasi Profesi Network Engineer Skema Network+ Bersama PT. Nusanet dan PT. Wilearning Indonesia," Jurnal Umum Pengabdian Masyarakat (JUPEMAS), vol. 1, no. 2, pp. 43–49, 2023.

W. Sulistyo and S. Sartomo, "Model Keamanan Jaringan Menggunakan Firewall Port Blocking," Krea-TIF J. Tek. Inform., vol. 10, no. 1, pp. 10–18, 2022, doi: 10.32832/kreatif.v10i1.6678.

"Vol. 10 No. 2 (2022): Desember 2022," vol. 10, no. 2, 2023.

R. N. Dasmen, M. Hendra Firmansyah, M. Khadafi, and Tri Yolanda, "Penerapan Keamanan Jaringan Menggunakan Metode Firewall Security Port," Decod. J. Pendidik. Teknol. Inf., vol. 2, no. 1, pp. 1–7, 2022, doi: 10.51454/decode.v2i1.29.

F. Timang, V. Bin Djusmin, and A. Anas, "Implementasi Keamanan Jaringan Menggunakan Web Proxy Pada Dinas Kebersihan Lingkungan Hidup Kota Palopo," no. 2, pp. 41–52, 2023.

N. Di, J. Komputer, R. R. Suleman, I. A. Salihi, and W. Yunus, "Penerapan Proxy Server Pada Mikrotik Untuk Blocking Situs," vol. 3, no. 2, pp. 49–56, 2024.

D. Firewall et al., "Implementasi Keamanan Hotspot Menggunakan Proxy," J. Ilm. Rekayasa dan Manaj. Sist. Inf., vol. 8, no. 2, pp. 148–154, 2022.

M. B. Yel, D. I. Mulyana, J. R. F, M. D. Nurfaishal, and M. H. T. B, "Optimalisasi Keamanan Firewall Pada Infrastruktur Jaringan Smk Idn Bogor," J. Cahaya Mandalika, vol. 4, no. 1, pp. 594–610, 2023, [Online]. Available: https://www.ojs.cahayamandalika.com/index.php/JCM/article/view/1393

B. Cahya, F. Rizki, A. Sutiyo, Y. El Saputra, and M. Elfarizi, "Implementasi Firewall Pada Mikrotik Untuk Keamanan Jaringan," J. JOCOTIS-Journal Sci. Inform. Robot. E, vol. 1, no. 2, pp. 63–80, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

F. P. Eka Putra, Amir Hamzah, W. Agel, and R. O. Firmansyah Kusuma, "Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking," J. Sistim Inf. dan Teknol., vol. 5, no. 4, pp. 82–87, 2024, doi: 10.60083/jsisfotek.v5i4.329.