Pembatasan Hak Akses Dengan Menggunakan *web proxy* Berbasis Mikrotik

Karisma Angeria*[1], A.R. Walad Mahfuzhi[2]
[1,2]Universitas Muhammadiyah Bengkulu ; Jl. Bali, Kampung Bali, Teluk Segara, Kota Bengkulu, 38119
[3]Program Studi Teknik Informatika, Universitas Muhammadiyah Bengkulu, Bengkulu
e-mail: ***[1]karismaanggelia562@gmail.com**, [2]walad@umb.ac.id

Abstrak

Seiring dengan pesatnya perkembangan teknologi jaringan komputer, pengguna kini dapat mengakses jaringan dengan lebih cepat dan efisien. Namun, di balik kemudahan akses internet, muncul masalah baru, yakni kemudahan dalam mengakses situs-situs negatif yang dianggap kurang bermanfaat bagi pengguna. Beberapa di antaranya adalah situs pornografi, situs yang mengandung konten kekerasan, serta situs perjudian yang semakin meningkat. Penelitian ini bertujuan untuk menciptakan internet yang lebih sehat dengan cara menerapkan pembatasan hak akses pada situs negatif, membatasi dan mengontrol akses internet, serta meningkatkan keamanan dan efisiensi jaringan untuk mencegah penyalahgunaan akses. Metode yang digunakan dalam penelitian ini adalah metode Experiment Oriented, yang bertujuan untuk menguji penerapan sistem pembatasan hak akses menggunakan perangkat MikroTik dalam jaringan komputer. Tahapan pelaksanaan penelitian ini meliputi identifikasi masalah, perancangan, penerapan, dan tahap pengujian. Hasil penelitian menunjukkan bahwa penerapan web proxy berbasis MikroTik di Laboratorium Komputer Fakultas Teknik Universitas Muhammadiyah Bengkulu efektif dalam meningkatkan keamanan jaringan. web proxy ini berhasil menerapkan pembatasan hak akses terhadap 26 situs yang tidak bermanfaat, seperti situs pornografi dan perjudian. Selain itu, konfigurasi ini juga membantu membatasi akses ke situs yang tidak relevan dengan tujuan akademik, sehingga menciptakan lingkungan jaringan yang lebih aman dan terkontrol.

Kata kunci*— Pembatasan akses, web proxy, Situs Negatif, Mikrotik dan Keamanan jaringan*

Abstract

Along with the rapid development of computer network technology, users can now access the network more quickly and efficiently. However, behind the ease of internet access, a new problem has emerged, namely the ease of accessing negative sites that are considered less useful for users. Some of these are pornographic sites, sites containing violent content, and increasingly gambling sites. This research aims to create a healthier internet by implementing restrictions on access rights on negative sites, limiting and controlling internet access, and increasing network security and efficiency to prevent misuse of access. The method used in this research is the Experiment Oriented method, which aims to test the implementation of a system for limiting access rights using MikroTik devices in computer networks. The stages of implementing this research include problem identification, design, implementation, and testing stages. The research results show that the implementation of a MikroTik-based web proxy in the Computer Laboratory of the Faculty of Engineering, Muhammadiyah University of Bengkulu is effective in improving network security. This web proxy succeeded in limiting access rights to 26 useless sites, such as pornography and gambling sites. Additionally, this configuration also helps limit access to sites that are not relevant to academic purposes, thereby creating a more secure and controlled network environment.

Keywords— *Access restrictions, web proxies, Negative Sites, Mikrotik and Network Security*

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer saat ini berkembang dengan sangat pesat, mencakup berbagai aspek baik perangkat keras maupun perangkat lunak yang mendukung operasionalnya. Jaringan komputer telah menjadi bagian penting dalam kehidupan sehari-hari karena hampir semua orang membutuhkan akses yang cepat dan efisien untuk memperoleh informasi melalui internet. Dengan menggunakan perangkat seperti komputer, laptop, atau ponsel, kita dapat tetap terhubung ke dunia luar dan mendapatkan informasi secara *real-time* tanpa hambatan jarak maupun waktu [1]. Selain itu, jaringan komputer juga menjadi suatu layanan yang sangat penting dengan manfaat yang jauh lebih besar dibandingkan dengan penggunaan komputer secara individual. Jaringan memungkinkan berbagai perangkat keras dan perangkat lunak, termasuk data, untuk digunakan bersama oleh banyak pengguna, sehingga meningkatkan efisiensi dan kolaborasi dalam berbagai kegiatan [2]. Keberadaan jaringan internet memberikan manfaat yang sangat besar bagi berbagai aktivitas manusia, mulai dari bidang pendidikan, di mana siswa dan guru dapat mengakses sumber belajar secara daring, hingga bidang pekerjaan, di mana kolaborasi jarak jauh menjadi lebih mudah dengan adanya *platform* komunikasi dan penyimpanan data berbasis *cloud*. Selain itu, di bidang hiburan, jaringan komputer memungkinkan kita untuk menikmati berbagai konten digital seperti video *streaming*, *game online*, atau musik kapan saja dan di mana saja. Kemajuan ini tidak hanya mempercepat alur informasi tetapi juga mendorong transformasi dalam cara manusia bekerja, belajar, dan bersosialisasi di era digital ini.

Pesatnya perkembangan teknologi internet tidak hanya memberikan kemudahan dalam mengakses informasi, tetapi juga membuka peluang bagi siswa untuk dengan mudah mengunjungi situs-situs yang seharusnya tidak mereka akses, seperti situs pornografi, perjudian, dan sejenisnya [3]. Masalah ini semakin diperburuk oleh kenyataan bahwa banyak remaja belum memahami cara menggunakan internet dengan bijak, sehingga mereka rentan terpengaruh oleh berbagai hal negatif. Selain pornografi dan perjudian, mereka juga sering kali terjebak dalam penggunaan media sosial yang tidak pantas, seperti mengumbar ranah pribadi, menyebarkan berita palsu, menjadi korban atau pelaku penipuan daring, hingga menghabiskan waktu dan uang pada permainan berbayar [4]. Hal ini menciptakan tantangan baru, yakni kemudahan akses terhadap konten yang tidak pantas dapat semakin memperburuk dampak negatif pada perkembangan mental dan moral pengguna, terutama di kalangan remaja [5].

MikroTik adalah sistem perangkat lunak yang dapat digunakan sebagai router jaringan yang handal. Sistem ini menawarkan beragam fitur lengkap yang mendukung kebutuhan jaringan kabel dan nirkabel, sehingga sangat fleksibel untuk berbagai konfigurasi jaringan [6]. MikroTik menawarkan Berbagai fitur yang dapat digunakan, seperti firewall dan web proxy [3]. *Web proxy* bertindak sebagai penghubung antara klien dan server, sehingga menghindari komunikasi langsung antara pengguna dan server internet untuk meningkatkan keamanan dan kontrol akses [7].

Untuk membatasi akses ke situs *web* yang mengandung konten negatif seperti pornografi, *web proxy* digunakan untuk memblokir atau memfilter konten – konten tersebut [1]. Selain itu *web proxy* memiliki kemampuan untuk memblokir situs secara efektif. Dengan cara mengatur konfigurasi pada router mikrotik, Setiap perangkat yang terhubung ke router itu akan secara otomatis memblokir akses ke situs-situs yang telah ditetapkan dalam pengaturan [8]. Secara keseluruhan, *web proxy* tidak hanya berfungsi sebagai alat pengendali akses, tetapi juga sebagai solusi untuk meningkatkan efisiensi, keamanan, dan pengelolaan jaringan secara keseluruhan.

Pada penelitian terdahulu yang dilakukan oleh [9] Penelitian ini mengkaji kurangnya keamanan jaringan akibat tidak digunakannya fitur *firewall* untuk menyaring paket data berdasarkan alamat IP. Metode yang digunakan adalah pendekatan kualitatif. Hasil Penelitian ini menunjukkan bahwa penerapan *web proxy* mampu meningkatkan keamanan jaringan secara optimal melalui pembatasan akses ke situs-situs tertentu yang berpotensi membahayakan pengguna. Adapun penelitian serupa [10] Tantangan utama yang dihadapi adalah meningkatnya ancaman terhadap keamanan jaringan dan kebutuhan untuk mengelola akses internet dengan lebih efisien di berbagai area. Metode penelitian yang digunakan Studi Pustaka, Identifikasi Kebutuhan, Perancangan Sistem, implementasi dan pengujian sistem. Penelitian ini membuktikan bahwa penggunaan kombinasi *DNS AdGuard* dengan Mikrotik Routerboard adalah alternatif yang efektif untuk meningkatkan keamanan serta efisiensi jaringan. Penelitian terkait lainnya [11] Pengelolaan jaringan internet di SMK Negeri 3 Seluma belum optimal, ditandai dengan akses bebas tanpa kontrol bagi guru, staf, dan siswa. Penelitian ini menggunakan metode PPDIO, yang meliputi *Prepare, Plan, Design, Implement, Operate* dan *Optimize*. Hasil penelitian menunjukkan bahwa penerapan *proxy* server dapat meningkatkan kinerja jaringan dengan membatasi akses ke situs-situs yang berpotensi mengandung virus atau malware. Adapun penelitian terdahulu [12] Masalah utama yang dihadapi adalah penyalahgunaan internet oleh oknum untuk kegiatan ilegal, seperti penyebaran pornografi, penipuan, dan perdagangan barang terlarang. Hal ini dapat memberikan dampak negatif, terutama pada anak-anak dan masyarakat umum. Penelitian ini menggunakan metode kualitatif. Hasil penelitian menunjukkan bahwa penggunaan Raspberry Pi untuk menganalisis *web proxy* efektif dan sesuai dengan hasil pengujian yang dilakukan. Penelitian serupa lainnya [13] Masalah yang dihadapi adalah akses terhadap materi yang tidak sesuai untuk semua kalangan, seperti pornografi, judi, dan konten kekerasan, yang tidak sejalan dengan budaya pengguna. Penelitian ini menggunakan metode kualitatif. Hasil pengujian menunjukkan bahwa sistem berfungsi dengan baik, mampu membatasi akses ke situs sesuai jadwal, dan halaman pemantauan bekerja sesuai kebutuhan. Adapun penelitian lainnya [14] Masalah yang dihadapi adalah penyusupan *cracker* melalui port-port jaringan yang dapat merugikan pemilik server dan jaringan.

Organisasi menggunakan jaringan untuk bertukar informasi dalam berbagai bentuk, namun risiko keamanan tetap ada. Penelitian ini menggunakan metode observasi lapangan, studi literatur, persiapan, pengujian, serta hasil dan rekomendasi. Hasil penelitian menunjukkan bahwa *web proxy* MikroTik efektif dalam mengatur pembatasan waktu akses dan memblokir situs yang tidak diinginkan. Penelitian terkait lainnya [15] Masalah yang dihadapi adalah adanya situs *web* bermuatan negatif yang dapat diakses melalui layanan internet, yang dapat membahayakan pengguna. Penelitian ini menggunakan metode identifikasi masalah, studi literatur, analisis kebutuhan, desain, konfigurasi, dan pengujian sistem. Hasil pengujian menunjukkan bahwa sistem *web filtering* dengan metode *DNS Forwarding* efektif dalam mengurangi akses ke situs bermuatan negatif saat pengguna terhubung ke internet. Adapun penelitian terdahulu lainnya [16] Masalah yang dihadapi Pembangunan Perumahan (Persero) Jakarta adalah penurunan kinerja jaringan internet akibat kurangnya pemantauan dan pembatasan akses ke situs yang mengganggu. Penelitian ini menggunakan metode pengumpulan data, analisis kebutuhan, desain, pengujian, dan implementasi. Hasil penelitian menunjukkan bahwa pembatasan akses internet atau pemblokiran situs efektif mengurangi penggunaan *bandwidth* berlebih, sehingga jaringan lebih stabil. Penelitian saat ini akan merinci langkah-langkah teknis untuk mengonfigurasi router Mikrotik, serta metode yang digunakan untuk mengukur efektivitas pemfilteran situs-situs negatif. Dengan demikian, penelitian ini bertujuan untuk memastikan bahwa sistem pemblokiran dapat berjalan dengan baik dan memberikan perlindungan yang efektif bagi pengguna, terutama anak muda, dalam mengakses informasi di internet.

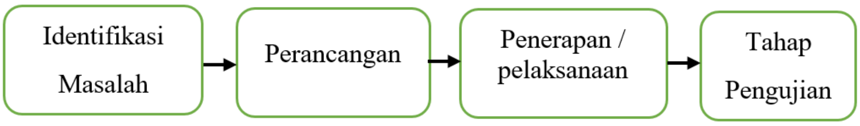
Berdasarkan uraian latar belakang maupun penelitian yang pernah dilakukan sebelumnya, Penelitian ini bertujuan untuk menerapkan dan menguji sistem pembatasan hak akses menggunakan perangkat Mikrotik dalam jaringan komputer, dengan fokus pada kontrol akses pengguna dan pengaturan kebijakan jaringan yang lebih efisien. Selain itu, penelitian ini juga bertujuan untuk menyediakan solusi yang dapat membatasi dan mengontrol akses internet bagi pengguna jaringan, khususnya di lingkungan Laboratorium Komputer Fakultas Teknik Universitas Muhammadiyah Bengkulu, untuk meningkatkan keamanan, efisiensi penggunaan jaringan, serta meminimalkan potensi penyalahgunaan akses internet.

2. METODE PENELITIAN

Dalam penelitian ini, metode yang digunakan adalah *Experiment Oriented*, yang bertujuan untuk menguji penerapan sistem pembatasan hak akses menggunakan perangkat Mikrotik dalam jaringan komputer. *Experiment Oriented* adalah metode penelitian yang berfokus pada pengujian hipotesis melalui eksperimen yang dirancang secara sistematis. Penelitian ini melibatkan konfigurasi Mikrotik untuk membatasi akses berdasarkan kategori konten, dan alamat *IP Address*. Eksperimen dilakukan pada jaringan lokal Laboratorium Fakultas Teknik Universitas Muhammadiyah Bengkulu untuk mencerminkan kondisi nyata. Data yang dikumpulkan mencakup tingkat keberhasilan dalam memblokir akses ke situs yang tidak diizinkan. Metode ini dipilih karena penelitian ini berfokus pada penerapan solusi teknis yang dapat diuji secara langsung dan terukur melalui eksperimen yang terstruktur. Pengujian dilakukan di lingkungan nyata untuk memperoleh data yang akurat mengenai efektivitas sistem pembatasan hak akses yang diterapkan menggunakan perangkat Mikrotik.

2.1 Tahap pelaksanaan

Adapun tahap pelaksanaan yang dilakukan pada penelitian dengan menggunakan *Experiment Oriented* yang ada pada gambar 1. Tahap Pelaksanaan.



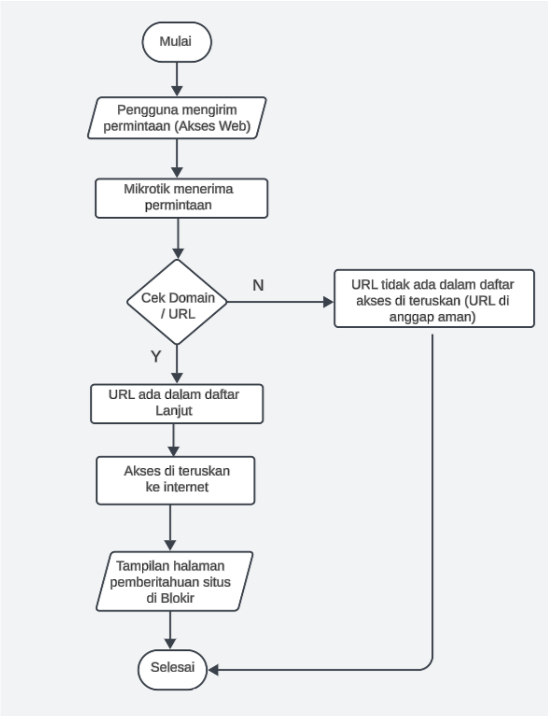
Gambar 1. Tahap pelaksanaan

1) Identifikasi permasalahan
   Pada tahap ini berupa identifikasi masalah, pengumpulan data/Observasi serta persiapan kebutuhan baik berupa perangkat keras maupaun perangkat lunak untuk melakukan konfigurasi *filtering* menggunakan *web proxy*. Observasi dilakukan melalui pengamatan langsung pada Laboratorium Komputer Fakultas Teknik Universitas Muhammadiyah Bengkulu, untuk mengidentifikasi permasalahan yang ada pada sistem jaringan yang sedang berjalan.
2) Perancangan
   Pada tahap ini, peneliti merancang topologi jaringan yang akan digunakan dalam eksperimen dengan menggunakan aplikasi desain topologi seperti *Cisco Packet Tracer*. Desain ini mencakup perangkat jaringan yang saling berhubungan, serta penempatan router Mikrotik sebagai *web proxy* untuk mengelola dan mengoptimalkan kontrol akses internet. Pembuatan desain ini bertujuan untuk memberikan gambaran bagaimana Mikrotik dapat diimplementasikan dalam jaringan dan menguji kinerjanya dalam meningkatkan efisiensi jaringan.
3) Penerapan
   Pada tahap ini, peneliti melakukan penerapan dari desain topologi jaringan yang telah direncanakan sebelumnya. Proses ini dimulai dengan pengaturan perangkat jaringan sesuai dengan desain, diikuti dengan konfigurasi *web proxy* pada perangkat Mikrotik menggunakan winbox.
   Penerapan ini mencakup pengaturan *filtering* untuk membatasi akses ke situs-situs tertentu serta pemblokiran konten yang tidak sesuai dengan kebijakan jaringan. Peneliti juga memastikan bahwa semua perangkat terhubung dengan benar dan pengaturan Mikrotik berjalan sesuai dengan tujuan.
4) Tahap pengujian
   Pada tahap ini dilakukan pengujian terhadap hasil konfigurasi *web proxy*. Pengujian dimulai dengan memantau koneksi internet dan menguji apakah konfigurasi *web proxy* yang telah diterapkan berhasil dalam mengelola akses ke situs-situs tertentu, sesuai dengan kebijakan yang telah ditetapkan. Pengujian dilakukan dengan mengakses berbagai situs

web untuk mengevaluasi efektivitas *filtering* dan pemblokiran konten, serta memastikan bahwa kontrol akses berjalan dengan baik tanpa gangguan. Data yang diperoleh selama pengujian akan dianalisis untuk mengetahui sejauh mana *web proxy* Mikrotik dapat memberikan solusi terhadap masalah yang diidentifikasi sebelumnya.

2.2 Flowchart Pembatasan Akses / Blokir situs web Proxy

Adapun Alur teknik manajemen hak akses atau pemblokiran situs yang dilakukan dapat di lihat pada Gambar 2, *Flowchart* Pembatasan Hak Akses / Blokir Situs



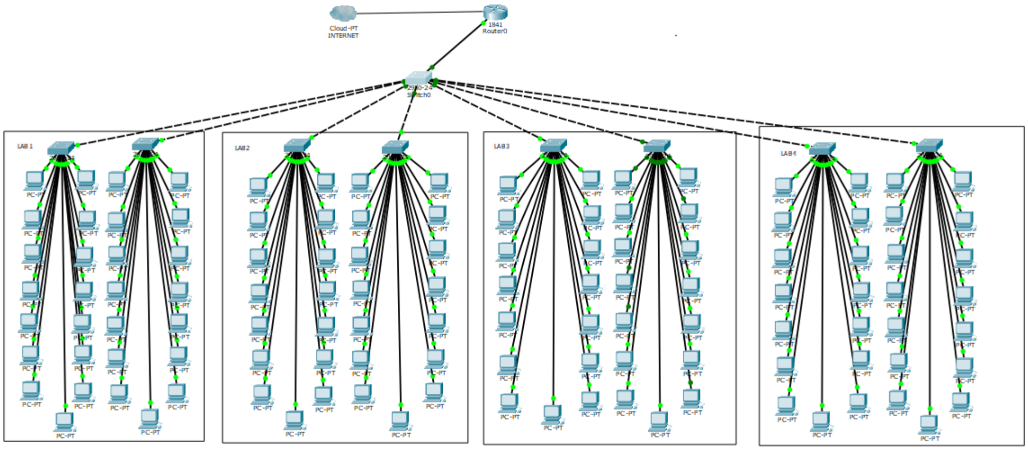
Gambar 2. *Flowchart* Pembatasan Hak Akses / Blokir Situs

Terlihat pada *Flowchart* Gambar 2, bahwa setiap permintaan akses *web* oleh klien akan diperiksa terlebih dahulu, apakah *URL* yang diminta termasuk dalam daftar yang diperbolehkan atau tidak. Jika permintaan klien mengarah ke situs *web* yang ada dalam daftar *URL* yang diblokir, maka akses akan diblokir, dan klien akan menerima tampilan bahwa situs *web* tersebut telah diblokir oleh administrator jaringan. Sebaliknya, jika permintaan klien mengarah ke situs yang tidak tercantum dalam daftar blokir, maka situs tersebut dianggap aman dan akses ke situs *web* dapat diteruskan.

3. HASIL DAN PEMBAHASAN

Dalam penelitian yang telah di lakukan di Laboratorium Komputer pada Fakultas Teknik Universitas Muhammadiyah Bengkulu, menujukkan bahwa masih adanya mahasiswa yang menggunakan komputer untuk suatu hal yang tidak bermanfaat seperti membuka *youtube*, *Instagram*, dan alamat situs lainnya.

Oleh karena itu peneliti mengusulkan penambahan konfigurasi pada mikrotik untuk meningkatkan dan mengoptimalkan keamanan jaringan pada Laboratorium Komputer Fakultas Teknik Universitas Muhammadiyah Bengkulu, terutama dalam memfilter konten atau situs internet yang tidak bermanfaat bagi aktivitas belajar, sehingga para mahasiswa dapat menggunakan internet dengan bijak dan lebih bermanfaat lagi.berikut merupakan topologi dan tabel kebutuhan yang di gunanakan dalam penerapan konfigurasi *web proxy*:



Gambar 3. Topologi jaringan

Tabel 1. Kebutuhan topologi jaringan

No	Nama Perangkat	Jumlah
1	Mikrotik	1 buah
2	Switch	9 buah
3	PC	120 buah

Pada topologi jaringan Gambar 3, Mikrotik digunakan sebagai router utama yang menghubungkan jaringan lokal dengan internet melalui dua *interface* . *Ether*1, yang terhubung ke sumber internet, diberi nama INTERNET dan dikonfigurasi untuk mendapatkan *IP Address* secara dinamis melalui *DHCP Client* dari *ISP*. *Ether*2, yang terhubung ke jaringan lokal, diberi nama LAB dengan *IP Address* statis 10.10.10.1/26, bertugas melayani perangkat-perangkat di subnet tersebut.

3. 1 Dasar Pengumpulan Data Situs Yang di Blokir

Dasar pengumpulan data situs yang diblokir di Laboratorium Fakultas Teknik Universitas Muhammadiyah Bengkulu didasarkan pada kebijakan institusi untuk menciptakan lingkungan belajar yang kondusif serta mencegah akses ke situs yang tidak relevan atau berbahaya. Situs yang menjadi target blokir meliputi kategori seperti media sosial, *streaming*, hiburan, serta konten negatif seperti pornografi dan perjudian. Situs media sosial seperti *Youtube*, *Instagram*, dan *Facebook* diblokir karena dapat mengalihkan perhatian mahasiswa dari kegiatan belajar, menurunkan produktivitas, serta meningkatkan penggunaan *bandwidth* secara signifikan, yang dapat mengganggu akses jaringan untuk kebutuhan akademik. Metode pengumpulan data mengacu pada daftar situs *blacklist* yang tersedia dari sumber eksternal, yang telah dikategorikan berdasarkan jenis konten dan tingkat risikonya. Dengan pendekatan ini, pembatasan hak akses menggunakan *web proxy* berbasis MikroTik dapat diterapkan secara efektif untuk mendukung kegiatan akademik di laboratorium.

Tabel 2. Daftar situs kategori Media Sosial, *Streaming* dan Hiburan yang di Blokir

No	Alamat *website*	status	Hasil pengujian
1	*Youtube*.com	*Deny*	Sukses
2	*Facebook*.com	*Deny*	Sukses
3	*Instagram*.com	*Deny*	Sukses
4	*Twitter*.com	*Deny*	Sukses

No	Alamat *website*	status	Hasil pengujian
5	*Netflix*.com	*Deny*	Sukses
6	*Spotify*.com	*Deny*	Sukses
7	*Disney+*.com	*Deny*	Sukses
8	*Snapchat*.com	*Deny*	Sukses
9	*Telegram*.com	*Deny*	Sukses

Tabel 3. Daftar situs kategori Pornografi yang di Blokir

No	Alamat *website*	status	Hasil pengujian
1	*Pornhub*.com	*Deny*	Sukses
2	*xvideos*.com	*Deny*	Sukses
3	*xnxx*.com	*Deny*	Sukses
4	*Xhamster*.com	*Deny*	Sukses
5	*RedTube*.com	*Deny*	Sukses
6	*YouPorn*.com	*Deny*	Sukses
7	*Brazzers*.com	*Deny*	Sukses
8	*SpankWire*.com	*Deny*	Sukses

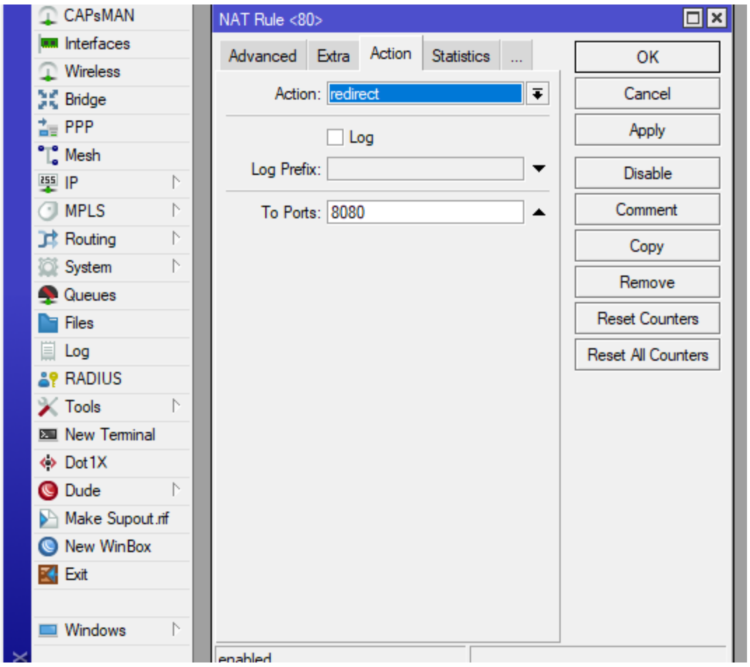
Tabel 4. Daftar situs kategori Perjudian yang di Blokir

No	Alamat *website*	status	Hasil pengujian
1	*bet365*.com	*Deny*	Sukses
2	*888poker*.com	*Deny*	Sukses
3	*William Hill*.com	*Deny*	Sukses
4	*Betfair*.com	*Deny*	Sukses
5	*Ladbrokes*.com	*Deny*	Sukses
6	*Ladbrokes*.com	*Deny*	Sukses
7	*Casino*.com	*Deny*	Sukses
8	*JackpotCity*.com	*Deny*	Sukses
9	togel.com	*Deny*	Sukses

3. 2 Konfigurasi web proxy

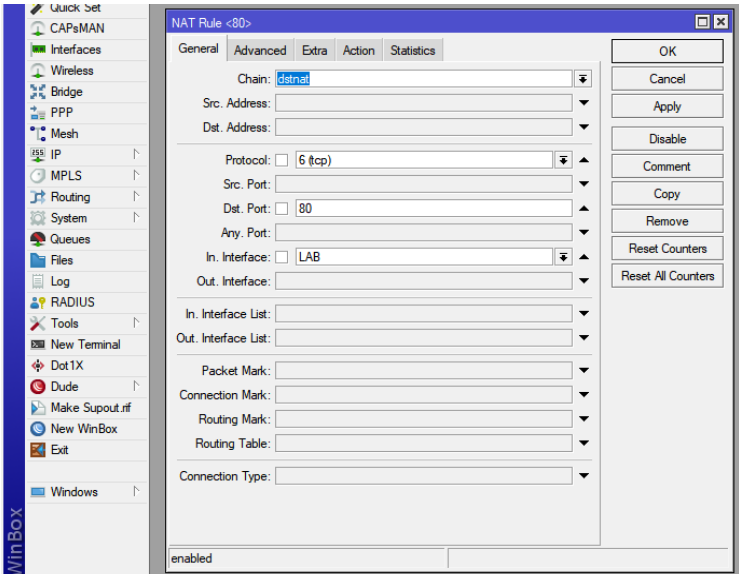
Untuk melakukan konfigurasi *web proxy* pada MikroTik, diperlukan perangkat lunak bernama Winbox sebagai pusat kontrol untuk mengakses server MikroTik. Adapun langkah – langkah konfigurasi *web proxy*.

1) Pertama buka aplikasi winbox untuk bisa melakukan *remote* pada mikrotik, setelah itu lakukan konfgurasi pemblokiran pada menu *web proxy*, dengan masuk ke bagian menu IP → *web proxy*, pada menu tab general centang *enable*, pada bagian port tuliskan angka 8080, angka ini menunjukkan nomor port yang digunakan untuk layanan *proxy HTTP*, pada bagian cache administrator tuliskan nama email yang bertanggung jawab atas pengelolaan cache atau *web proxy*, setelah itu pilih apply untuk menyimpan pengaturan ini. Proses konfigurasi ini dapat dilihat pada Gambar 4.



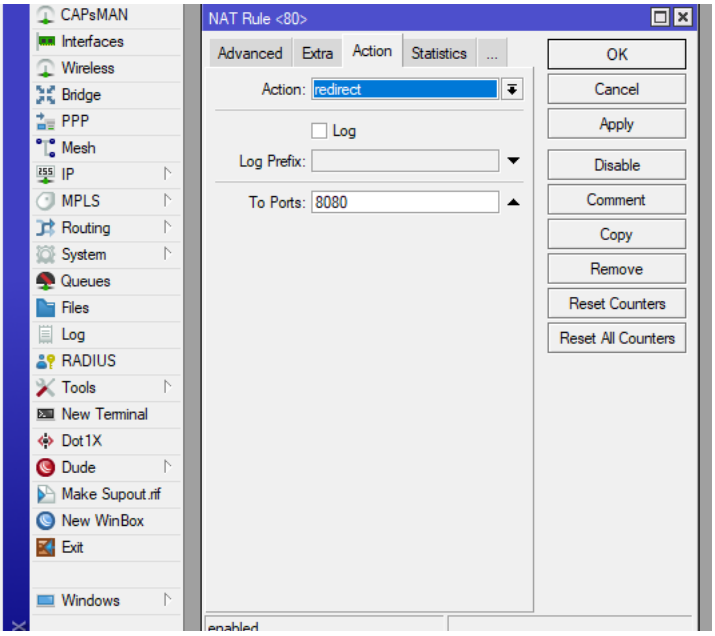
Gambar 4. *Setting web Proxy*

2) Setelah itu lakukan konfigurasi *Transparent proxy* pada menu IP → *Firewall* → *NAT*, klik tanda "+", pilih tab general, pastikan megisi chain dengan opsi dst*nat*, *protocol* pilih opsi 6(tcp), dst port di isi 80, setelah itu pada bagian in.*interface* pilih *interface* yang ingin di buat *Transparent proxy*. Proses konfigurasi ini dapat dilihat pada Gambar 5.



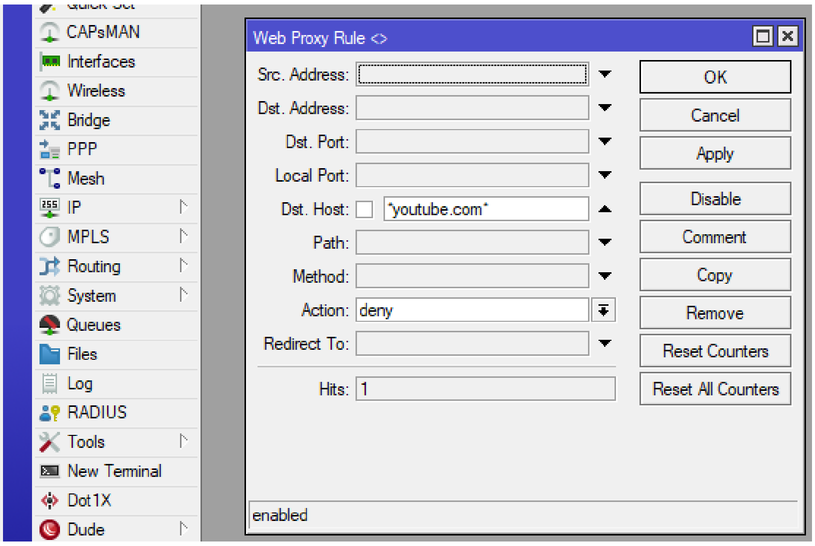
Gambar 5. *Setting* menu *NAT Rule*

Selanjutnya, pada tab *Action* pilih opsi redirect, lalu pada bagian to ports isi dengan angka 8080 sesuai dengan konfigurasi di menu *web Proxy*. Proses konfigurasi ini dapat dilihat pada Gambar 6.



Gambar 6. *Action NAT*

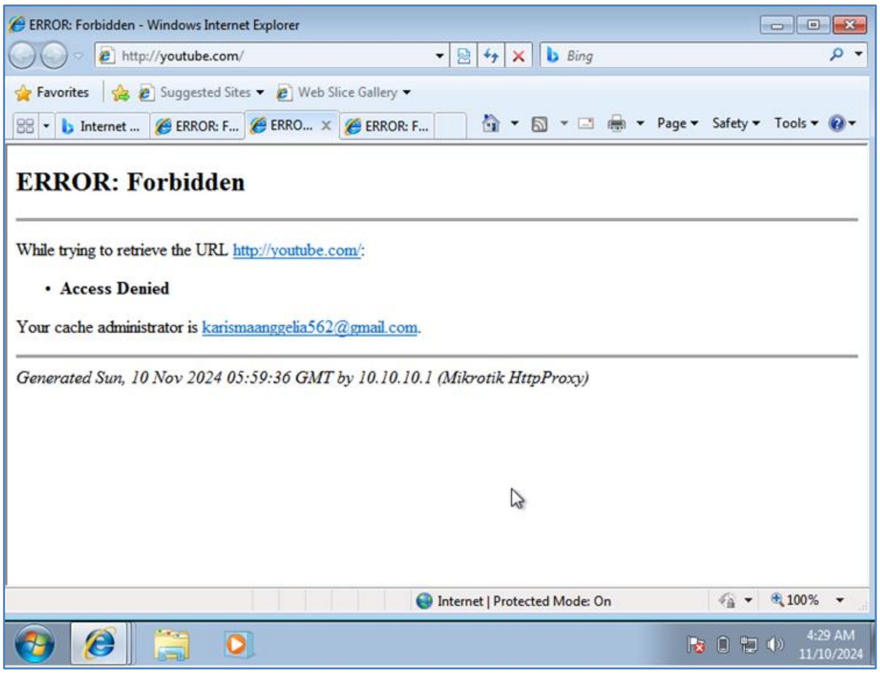
3) Selanjutnya, kembali ke menu *web proxy* dan masuk ke “Access” untuk menambahkan aturan blokir. Pada menu *web proxy* rule, klik “+” untuk membuat aturan baru. Di bagian “*dst host*”, isi dengan alamat situs yang ingin diblokir. Selanjutnya, pada bagian “*Action*”, pilih opsi *Deny* untuk memblokir atau menolak akses ke situs yang telah dicantumkan di bagian sebelumnya. Proses konfigurasi ini dapat dilihat pada gambar 7.



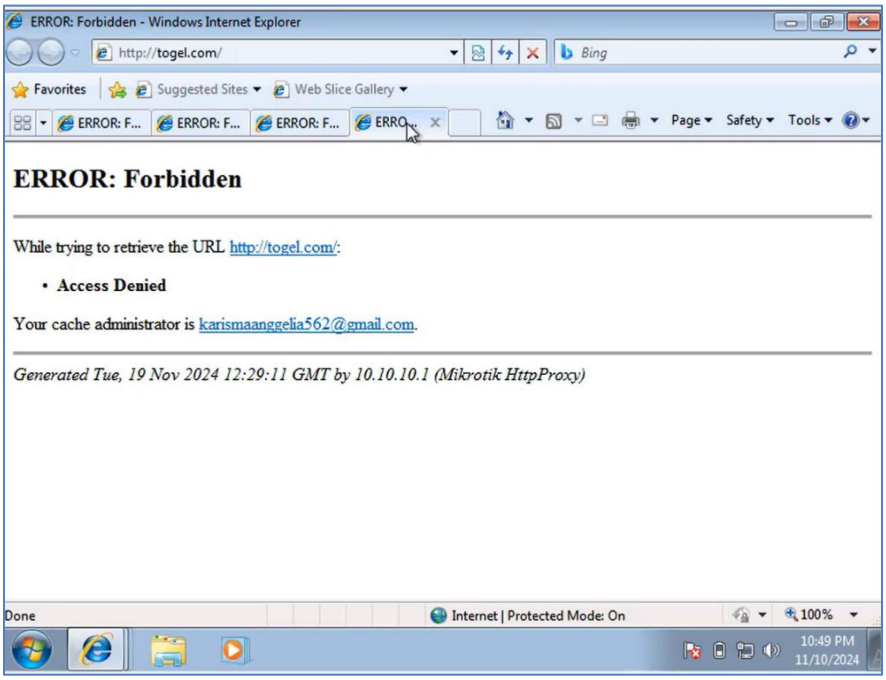
Gambar 7. *Setting* menu Access Blokir *web*

3. 3 Hasil Pengujian web proxy

Hasil pengujian konfigurasi *web proxy* menunjukkan keberhasilan penerapan aturan pemblokiran pada situs yang telah ditentukan. Pengujian memastikan bahwa situs yang diblokir tidak dapat diakses oleh pengguna, khususnya mahasiswa. Hasil pengujian ini menjadi acuan penting untuk menilai efektivitas konfigurasi *web proxy* dalam mencapai tujuan pemblokiran. Dari hasil ini, dapat dilihat bahwa aturan pemblokiran telah diterapkan secara konsisten dan efektif pada semua pengguna, yang menunjukkan bahwa konfigurasi telah berhasil. Hasil pengujian pemblokiran situs dapat dilihat pada Gambar 8 dan Gambar 9.



Gambar 8. Hasil pengujian blokir *youtube*.com



Gambar 9. Hasil pengujian blokir Togel.com

4. KESIMPULAN

Kesimpulan yang dapat diperoleh dari penelitian ini adalah sebagai berikut:

1. Dari hasil penelitian penerapan konfigurasi pada perangkat MikroTik di Laboratorium Komputer Fakultas Teknik Universitas Muhammadiyah Bengkulu, yang berhasil

memblokir 26 situs yang dianggap kurang bermanfaat, dapat disimpulkan bahwa implementasi *web proxy* berbasis MikroTik efektif dalam meningkatkan keamanan jaringan. Situs yang berhasil diblokir terdiri dari kategori media sosial, *streaming*, dan hiburan yang mencakup total 9 situs, kategori situs pornografi (8 situs), dan kategori perjudian (9 situs). Dengan demikian, implementasi *web proxy* ini efektif dalam memblokir situs berbahaya dan membatasi akses ke situs yang tidak relevan dengan pembelajaran.
2. Kelebihan penelitian ini adalah kemampuan konfigurasi *web proxy* MikroTik dalam meningkatkan keamanan dan efisiensi jaringan dengan memblokir situs yang tidak relevan, sehingga pengguna dapat lebih fokus pada pembelajaran dan mengurangi potensi penyalahgunaan internet.
3. Kelemahan penelitian ini adalah keterbatasan dalam cakupan pemblokiran yang hanya mencakup situs-situs tertentu, seperti media sosial, pornografi, dan perjudian, serta pengujian yang terbatas pada satu laboratorium, sehingga hasilnya belum tentu berlaku untuk jaringan yang lebih luas atau jumlah pengguna yang lebih banyak.

5. SARAN

Saran untuk pengembangan penelitian selanjutnya adalah sebagai berikut:
1. Penelitian selanjutnya dapat fokus pada implementasi konfigurasi *web proxy* di berbagai lingkungan yang lebih luas, seperti di tingkat sekolah, universitas, atau organisasi, untuk mengevaluasi efektivitas pengaturan akses internet dalam skala yang lebih besar.
2. Penelitian lanjutan dapat mengkaji pengembangan dan otomatisasi pembaruan daftar situs yang diblokir, dengan memanfaatkan teknologi yang lebih canggih untuk menjaga relevansi dan efektivitas pengaturan seiring dengan munculnya ancaman baru.
3. Fokus penelitian selanjutnya dapat diarahkan pada pengembangan metode baru yang lebih efektif dalam meningkatkan keamanan dan efisiensi jaringan, termasuk eksplorasi algoritma atau teknik baru untuk deteksi dan pencegahan akses ke situs berbahaya.

UCAPAN TERIMA KASIH

Penulis mengucapkan syukur yang sebesar-besarnya kepada Allah SWT atas limpahan rahmat, hidayah, dan kemudahan yang diberikan sehingga artikel ini dapat diselesaikan dengan baik. Penulis juga menyampaikan rasa terima kasih yang mendalam kepada orang tua tercinta atas doa, dukungan moral, dan kasih sayang yang tak pernah putus. Ucapan terima kasih disampaikan kepada seluruh pihak yang telah memberikan dukungan, bimbingan, dan masukan selama proses penyusunan artikel ini, khususnya kepada Universitas Muhammadiyah Bengkulu atas bantuan berupa materi dan fasilitas yang telah di sediakan. Terima kasih juga disampaikan kepada dosen pembimbing Bapak A.R.Walad Mahfuzhi, S.Kom., M.Kom., yang telah memberikan arahan serta masukan yang sangat berharga, serta sahabat-sahabat terdekat yang selalu memberikan semangat dan motivasi dalam setiap langkah penulis.

DAFTAR PUSTAKA

[1] M. Noviansyah and H. Saiyar, 2020, "Pemanfaatan *web proxy* Sebagai Pengoptimal Keamanan," *J. Khatulistiwa Inform.*, no. 1, vol. VIII, pp. 34–39, Doi: *HTTP*s://doi.org/10.31294/jki.v8i1.8356 .

[2] *F. M. Naufal, M. R. Vahlevi, A. Widayana, M. L. Zulfa, and D. Juardi,* 2022, "Implementasi Keamanan Hotspot Menggunakan *Proxy*," *J. Ilm. Rekayasa dan Manaj. Sist. Inf.*, no. 2, vol. 8, pp. 148–154, Doi: *HTTP*://dx.doi.org/10.24014/rmsi.v8i2.17691

[3] M. A. Rozan, M. Tahir, A. P. Qirani, N. Rizqiullah, M. Veranda, R. Puji, and A. Ghaffar,

2024, “Implementasi *web proxy* Pada Mikrotik Untuk Mengoptimalkan Keamanan Jaringan Wireless Lan Di Lingkungan Sekolah Man 1 Gresik,” *J. Pendidik. Teknol. Inf.*, no. 1, vol. 7, pp. 180–188, doi: 10.37792/jukanti.v7i1.1280.

[4] A. Siswopranoto, A. Ikhsan, G. Saputri, I. Aisyah, and R. Ester, 2021, “Sosialisasi Internet Sehat Di Kalangan Remaja Untuk Meminimalkan Dampak Negatif Dari Berinternet Pada SMP Islam Al Wasatiyah,” *J. Ilmu Komput. JIK*, no. 2, vol. IV, pp. 44–49, *HTTP*s://jurnal.pra*NAT*aindonesia.ac.id/index.php/jik/article/view/100

[5] M. A. Abdilah, I. Alfiani, M. A. Ulbarokah, and K. W. Nugraha, 2021, “Optimasi Mikrotik Routerboard Sebagai Upaya Mewujudkan Internet Sehat,” *J. Tek. Inform. Dan Sist*,no.1,vol.1,pp.31–37,*HTTP*s://jurtisi.stmikmpb.ac.id/index.php/jurtisi/article/view/19

[6] Mhd. Ilham, Indra Gunawan, and Zulia Almaida Siregar, 2022, “Keamanan Jaringan Wlan Dengan Metode *Firewall Filtering* Menggunakan Mikrotik Pada Smp Negeri 1 Dolok Merawan,” *J. Ilm. Sist. Inf. dan Ilmu Komput.*, no. 3, vol. 2, pp. 01–16, doi: 10.55606/juisik.v2i3.309.

[7] T. Widyanto, N. Manurung, and S. Sahren, 2023, “External *Proxy* Menggunakan Router Mikrotik Dalam Optimasi *Bandwidth* Laboratorium Stmik Royal,” no. 3, vol. 3, pp. 175–180, Doi: *HTTP*s://doi.org/10.33330/jutsi.v3i3.2813

[8] S. Bahri, D. El, and R. Purba, 2022, “Implementasi *web proxy* Pada Mikrotik untuk Menciptakan Internet Sehat pada SMK Al Maksum Langkat,” *J. Tek. Inform. Unika ST. Thomas.*, No. 02 vol. 07, pp. 272–277, *HTTP*://ejournal.ust.ac.id/index.php/JTIUST/article/view/2425

[9] F. Timang, V. Bin Djusmin, and A. Anas, 2023, “Implementasi Keamanan Jaringan Menggunakan *web proxy* Pada Dinas Kebersihan Lingkungan Hidup Kota Palopo,” *J. Ilm. Tek. Inform.*, no. 2, Vol. 1,pp. 41–52,

[10] *M. A. N. Pratama and F. Thalib*, 2024, *Jurnal Teknologi dan Sistem Informasi*, “ Penerapan Sistem Keamanan Jaringan dengan *DNS AdGuard* ada Linux Debian dan Kontrol Akses Internet Berdasarkan Waktu Implementasi Pada Mikrotik Routerboard” no. 4, vol. 2, Doi: *HTTP*s://doi.org/10.61132/saturnus.v2i4.346

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

[12] Y. W. and Y. B. Fitriana, A. Susanto, E. S. Susanto, F. Hamdani, M. Rizky, and N. Oper, 2022, “Implemetasi *Filtering* Alamat *website* Pada *web Proxy*Menggunakan Raspberry-Pi,” no. 1, vol. 7, pp. 55–61, Doi: *HTTP*s://doi.org/10.30591/jpit.v7i1.3835

[13] H. Kurniawan, J. Dedy Irawan, and F. . Ariwibisono, 2020, “Implementasi Squid *Proxy* Pada Mikrotik Dan Monitoring Traffic Jaringan Berbasis *website*,” *JATI (Jurnal Mhs. Tek. Inform.*, no. 2, vol. 4, pp. 136–143, doi: 10.36040/jati.v4i2.2691.

[14] F. Idwara, S. Hamza, and J. Noh, 2024, "Sistem Keamanan Jaringan Komputer Menggunakan Metode Mac *Filtering* Dengan *web proxy* Dan Manajemen *Bandwidth* Di Sma Negeri 6 Kota Ternete," *J-TIFA:Jurnal Teknologi Informatika.*, no. 2, vol. 2617, pp. 7–16, DOI:*HTTP*s://doi.org/10.52046/j-tifa.v5i1.1349

[15] Randy Ikhsan Ramadhan and Siti Madinah Ladjamuddin, 2022, “Perancangan Sistem *web Filtering* Dengan Metode *DNS Forwarding* Pada Jaringan Komputer Berbasis Mikrotik Routeros,” *J. Inform. Dan Tekonologi Komput.*, no. 2, vol. 2, pp. 146–157, doi: 10.55606/jitek.v2i2.231.

[16] H. S. A. N. A. Ibrahim Fadilah Nawal, 2021, “Monitoring Jaringan Menggunakan Mikrotik Traffic Monitor Dan Metode *web proxy* Pada Pt. Pembangunan Perumahan (Persero) Jakarta,” *Monit. Jar. Menggunakan Mikrotik Traffic Monit. Dan Metod. web proxy Pada Pt. Pembang. Perumah. Jakarta*, vol. 7, no. 1, pp. 1–6, *HTTP*s://journal.uniku.ac.id/index.php/buffer.