JUTIK : Jurnal Teknologi Informasi dan Komputer
Oktober-2025, Vol. 11, No.2, Hal.175-185
ISSN(P): 2442-241X; ISSN(E): 2528-5211

IMPLEMENTANSI *MANGLE FILTERING CONTENT* MENGGUNAKAN MIKROTIK UNTUK MENINGKATKAN KEAMANAN JARINGAN

Aldo Bonifasius Simbolon[1*], Dean Siregar[2], Steven Adventino Gulo[3], Dedy Kiswanto[4]
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[1]
Email*: aldosimbolon017@gmail.com
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[2]
Email: deansiregar1609@gmail.com
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[3]
Email: stevenadventgulo@gmail.com
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[4]
Email: dedykiswanto@unimed.ac.id

(*) *Corresponding Author*

ABSTRAK

Keamanan jaringan menjadi aspek krusial yang harus diperhatikan dalam pengelolaan sistem informasi. Penelitian ini berfokus pada implementasi *Mangle Filtering Content* menggunakan perangkat MikroTik RB750 untuk meningkatkan keamanan jaringan. Metode eksperimen dengan pendekatan studi kasus digunakan untuk menguji efektivitas fitur *firewall mangle* dalam memblokir konten tidak diinginkan pada jaringan lokal. Penelitian dilakukan dengan merancang topologi jaringan sederhana yang terdiri dari *router* MikroTik sebagai pusat pengaturan lalu lintas, satu perangkat *client*, dan koneksi internet. Penerapan *mangle rules* dilakukan untuk menandai koneksi berdasarkan domain dan pola URL tertentu melalui *Layer-7 Protocol Filtering*, kemudian mengintegrasikan hasil *mangle* dengan *Filter Rules* untuk memblokir akses ke situs yang tidak diinginkan seperti media sosial dan situs dewasa. Hasil penelitian menunjukkan bahwa implementasi *mangle filtering content* pada MikroTik berhasil memblokir akses ke situs yang telah ditentukan, sehingga menciptakan lingkungan digital yang lebih aman dan terkontrol. Penelitian ini memberikan solusi praktis bagi administrator jaringan dalam meningkatkan keamanan dan pengelolaan konten digital pada jaringan skala kecil hingga menengah.
Kata kunci: *firewall*, keamanan jaringan, *mangle*, MikroTik, pemfilteran konten

ABSTRACT

Network security is a crucial aspect that must be taken into account in information system management. This research focuses on implementing Mangle Filtering Content using MikroTik RB750 device to enhance network security. An experimental method with a case study approach was used to test the effectiveness of the mangle firewall feature in blocking unwanted content on local networks. The research was conducted by designing a simple network topology consisting of a MikroTik router as the traffic control center, one client device, and an internet connection. Mangle rules were implemented to mark connections based on specific domains and URL patterns through Layer-7 Protocol Filtering, then integrating the mangle results with Filter Rules to block access to unwanted sites such as social media and adult websites. The results showed that the

Submitted: 14 April 2025
Accepted: 15 September 2025
Published: 10 Oktober 2025

implementation of mangle filtering content on MikroTik successfully blocked access to predetermined sites, creating a safer and more controlled digital environment. This research provides practical solutions for network administrators in improving security and digital content management on small to medium-scale networks.
Keywords: content filtering, firewall, mangle, MikroTik, network security

1. PENDAHULUAN

Keamanan jaringan menjadi aspek krusial yang harus diperhatikan dalam pengelolaan sistem informasi. Perkembangan teknologi informasi saat ini menjadi sesuatu yang sangat dibutuhkan oleh masyarakat. Hal ini karena teknologi mampu menjadi solusi atas berbagai tantangan di banyak bidang kehidupan [1]. Salah satu contoh nyata dari kemajuan tersebut adalah internet, sebuah sistem global yang menghubungkan jaringan komputer di seluruh dunia. Kini, internet tak hanya menghubungkan komputer, tetapi juga berbagai perangkat lainnya, melayani miliaran pengguna dari berbagai penjuru dunia [2]. Internet memberikan kemudahan bagi siapa pun untuk mencari dan mengakses informasi sesuai kebutuhan. Keberadaannya menjadi bukti konkret dari pesatnya perkembangan teknologi. Namun, dampak dari internet bisa bersifat positif maupun negatif, tergantung pada cara pengguna memanfaatkannya [3]. Sayangnya, kemudahan akses ini juga membuka peluang terhadap hal-hal yang bersifat negatif, seperti konten pornografi, *cyberbullying*, dan perjudian yang menjadi ancaman serius, terutama bagi remaja [4]. Di lingkungan sekolah, kebebasan dalam mengakses internet tanpa pengawasan yang memadai juga bisa membawa dampak buruk, seperti masuknya *malware, virus, spam, trojan,* dan berbagai serangan dari luar yang membahayakan sistem komputer [5]. Karena itu, isu keamanan menjadi sangat penting untuk diperhatikan, terutama di era digital yang serba cepat dan praktis seperti sekarang. Jaringan sebagai media komunikasi membutuhkan sistem keamanan yang andal untuk memberikan rasa aman dan mencegah berbagai ancaman yang tidak diinginkan, seperti serangan *virus* dan *spam* [6]. Untuk itu, diperlukan solusi yang efektif dalam melakukan penyaringan konten (*content filtering*) agar lalu lintas data yang melewati jaringan tetap aman dan terkendali. Salah satu metode yang dapat diterapkan adalah *Mangle Filtering Content* pada perangkat Mikrotik, yang memungkinkan administrator jaringan untuk memfilter konten berdasarkan parameter tertentu. Dalam penelitian terdahulu, dijelaskan bahwa penggunaan perangkat jaringan seperti Mikrotik sangat efektif dalam mengatur dan mengamankan lalu lintas data dengan memanfaatkan fitur-fitur yang ada, termasuk *mangle* dan *firewall* [7]. Penelitian ini berfokus pada bagaimana cara mengimplementasikan *Mangle Filtering Content* menggunakan Mikrotik untuk meningkatkan keamanan jaringan, seberapa efektif metode tersebut dalam menyaring konten berbahaya, dan bagaimana pengaruhnya terhadap kinerja jaringan secara keseluruhan. Tujuan dari penelitian ini adalah untuk mengimplementasikan metode *Mangle Filtering Content* pada perangkat Mikrotik sebagai upaya meningkatkan keamanan jaringan, mengevaluasi efektivitasnya dalam memblokir konten yang tidak diinginkan, serta memberikan solusi praktis bagi pengelola jaringan dalam menciptakan lingkungan digital yang lebih aman dan terkendali.

2. TINJAUAN PUSTAKA

MikroTik dan RouterOS

MikroTik RouterOS merupakan sistem operasi jaringan *open-source* yang menyediakan fitur lengkap untuk manajemen jaringan seperti *routing, firewall,* dan

bandwidth management [8]. Penelitian terdahulu oleh Asyiq Maulana dkk. menunjukkan bahwa implementasi *firewall* MikroTik melalui kombinasi *filter* dan *Raw Rules* berhasil memblokir akses konten tidak produktif seperti media sosial dan *streaming* di lingkungan sekolah dengan efektivitas 100% pada uji LOIC (*Denial of Service*). Kemampuan ini didukung arsitektur *stateful packet inspection* dan *Layer-7 protocol detection* yang memungkinkan identifikasi *traffic* berdasarkan protokol aplikasi. Penelitian lain menyebutkan bahwa mengimplementasikan MikroTik RouterOS dalam infrastruktur jaringan desa menggunakan metodologi NDLC (*Network Development Life Cycle*), menghasilkan sistem *monitoring bandwidth* dan peningkatan keamanan jaringan melalui konfigurasi *firewall* berbasis *address list* [9]. Penelitian ini mengonfirmasi fleksibilitas MikroTik dalam *environment* skala menengah dengan kemampuan manajemen terpusat melalui antarmuka WinBox. Kedua penelitian tersebut menggarisbawahi peran krusial fitur *Mangle* dalam RouterOS untuk melakukan *marking packet* dan modifikasi *header* IP, yang menjadi dasar implementasi *filtering content* dan manajemen QoS (*Quality of Service*). Kombinasi antara *firewall stateful*, *Layer-7 filtering*, dan *Mangle Rules* menjadikan MikroTik solusi komprehensif untuk keamanan jaringan berlapis.

Konsep Dasar Keamanan Jaringan

Keamanan jaringan adalah aspek fundamental dalam melindungi data, perangkat keras, perangkat lunak, dan layanan dari ancaman siber. Menurut penelitian yang ditulis oleh Reza [10] menyatakan bahwa keamanan jaringan bertujuan untuk menjaga validitas, integritas, dan ketersediaan data dalam sistem komputer. Salah satu pendekatan inovatif yang digunakan adalah metode *dynamic port knocking*, yang memastikan akses hanya diberikan kepada pengguna yang sah melalui mekanisme autentikasi berbasis *port* dinamis. Metode ini menggunakan teknologi enkripsi yang kuat untuk meningkatkan perlindungan terhadap sumber daya jaringan, meskipun memiliki tantangan seperti sinkronisasi waktu antara *client* dan *server* serta kompleksitas pengaturan sistem. Selain itu, penelitian oleh Widian [11] menekankan pentingnya *firewall* sebagai elemen utama dalam desain keamanan jaringan. *Firewall* berfungsi untuk mendeteksi dan merespons potensi serangan melalui pengamanan *port* serta pemantauan lalu lintas jaringan. Penelitian ini menunjukkan bahwa penerapan *firewall* secara optimal dapat meningkatkan efisiensi sistem sekaligus menjaga integritas data. Ketiga penelitian tersebut menyoroti pentingnya penerapan teknologi keamanan jaringan yang adaptif dan proaktif untuk menghadapi ancaman siber yang semakin kompleks. Dengan kombinasi metode seperti *firewall*, sistem deteksi intrusi berbasis AI, dan enkripsi dinamis dapat memastikan perlindungan menyeluruh terhadap aset digital mereka.

Filtering Konten dalam Jaringan Komputer

Filtering konten dalam jaringan komputer merupakan teknik penting untuk mengelola akses informasi dan melindungi pengguna dari konten yang tidak diinginkan. Penelitian oleh Munira [12] menjelaskan implementasi *web filtering* menggunakan DNS *forwarding* pada jaringan *wireless* berbasis MikroTik di SMA Negeri 1 Palopo. Penelitian ini menunjukkan bahwa dengan menerapkan konfigurasi DNS *forwarding*, administrator jaringan dapat mengontrol akses ke situs *web* berdasarkan kategori konten tertentu, seperti media sosial dan perjudian. Hasilnya, sistem ini berhasil meningkatkan keamanan dan produktivitas penggunaan internet di lingkungan sekolah dengan efisiensi pengawasan yang lebih baik. Implementasi ini menunjukkan bahwa penggunaan *firewall* tidak hanya efektif dalam memblokir akses ke situs berbahaya tetapi juga dalam

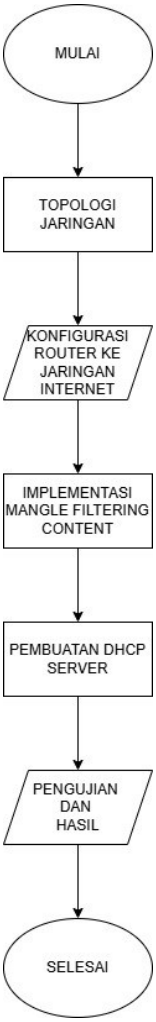
mengelola *bandwidth* secara efisien, sehingga mendukung kinerja jaringan secara keseluruhan. Lebih lanjut, penelitian oleh Muklas [13] membahas tantangan yang dihadapi dalam penerapan *filtering content*, termasuk kebutuhan untuk menjaga keseimbangan antara kebebasan akses informasi dan perlindungan terhadap konten berbahaya. Mereka menekankan pentingnya pendekatan yang adaptif dan berkelanjutan dalam pengembangan sistem filtering untuk memastikan bahwa solusi yang diterapkan tetap relevan dengan perkembangan teknologi dan jenis ancaman baru yang muncul. Penelitian-penelitian ini menegaskan bahwa filtering konten adalah komponen vital dalam strategi keamanan jaringan modern, memberikan perlindungan terhadap pengguna sambil memastikan penggunaan sumber daya jaringan yang optimal.

Firewall MikroTik dan Hubungannya dengan Mangle

Firewall MikroTik adalah komponen penting dalam pengelolaan keamanan jaringan, yang berfungsi untuk mengontrol akses dan melindungi sistem dari ancaman eksternal. Penelitian oleh Fitrian [14] menyoroti efektivitas penggunaan *firewall* MikroTik dalam filtering konten, khususnya untuk memblokir akses ke situs judi *online*. Dalam penelitian ini, penulis menerapkan metode konfigurasi *firewall filter rules* yang memungkinkan administrator untuk menetapkan aturan spesifik berdasarkan kata kunci atau URL. Hasil pengujian menunjukkan bahwa sistem berhasil menciptakan lingkungan digital yang lebih aman dengan memblokir akses ke konten yang tidak sesuai, yang menunjukkan relevansi penggunaan *firewall* dalam meningkatkan keamanan jaringan. Hubungan antara *firewall* MikroTik dan fitur *Mangle* juga sangat signifikan. *Mangle* berfungsi untuk menandai paket data yang melewati *router*, memungkinkan pengaturan lebih lanjut terhadap lalu lintas jaringan. Menurut penelitian oleh Hamza [15], penggunaan *Mangle* dalam pengaturan jalur paket data dapat dilakukan melalui fitur seperti *Mark Connection*, *Mark Packet*, dan *Mark Routing*. Fitur-fitur ini memberikan fleksibilitas dalam manajemen lalu lintas, termasuk pemilihan jalur routing berdasarkan kriteria tertentu, yang sangat penting dalam skenario di mana beberapa penyedia layanan internet (ISP) digunakan. Lebih lanjut, penelitian oleh Noviansyah [16] menunjukkan bahwa penerapan Mangle dapat meningkatkan efisiensi jaringan dengan mengoptimalkan penggunaan *bandwidth* melalui teknik *per connection queuing* (PCQ). Dengan mengatur prioritas paket berdasarkan tanda yang diberikan oleh *Mangle*, administrator dapat memastikan bahwa aplikasi kritis seperti video *conference* mendapatkan bandwidth yang cukup, sehingga meningkatkan kualitas layanan. Integrasi antara *firewall* MikroTik dan fitur *Mangle* menciptakan solusi keamanan yang komprehensif dan adaptif dalam manajemen jaringan. Penelitian-penelitian tersebut menegaskan bahwa kombinasi ini tidak hanya melindungi jaringan dari ancaman tetapi juga meningkatkan performa dan efisiensi operasionalnya.

3. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen dengan pendekatan studi kasus untuk menerapkan sistem pemfilteran konten berbasis *mangle* pada perangkat MikroTik RB750. Tujuan utama dari metode ini adalah menguji secara langsung efektivitas fitur *firewall mangle* dalam memblokir konten-konten tertentu yang tidak diinginkan dalam sebuah jaringan lokal. Objek penelitian dilakukan pada skenario jaringan berskala kecil, yang umum ditemukan di lingkungan rumah, sekolah, atau kantor kecil.



Gambar 1. Alur metode penelitian

Tahap awal penelitian dimulai dengan perancangan topologi jaringan. Jaringan terdiri dari satu *router* MikroTik RB750 sebagai pusat pengaturan lalu lintas, satu perangkat *client*, dan koneksi internet yang disediakan oleh penyedia layanan (ISP). Konfigurasi jaringan dasar seperti pengaturan IP *address*, NAT (*Network Address Translation*), DNS, dan DHCP *server* dilakukan terlebih dahulu untuk memastikan *client* dapat mengakses internet secara normal sebelum filter konten diterapkan.

Langkah selanjutnya adalah penerapan aturan *mangle*. Fitur ini digunakan untuk menandai koneksi atau paket yang berasal dari atau menuju situs-situs tertentu. Penandaan dilakukan berdasarkan alamat *domain*, *port*, ataupun pola URL tertentu yang didefinisikan menggunakan *Layer-7 Protocol*. Peneliti membuat beberapa aturan *mangle* untuk memisahkan jenis lalu lintas berdasarkan kategori konten, seperti sosial media, situs dewasa, atau situs judi *online*. Misalnya, *domain-domain* seperti chatgpt.com, youtube.com, atau otakudesu.cloud dimasukkan ke dalam pola *Layer-7* untuk dilakukan penandaan.

Setelah paket berhasil ditandai, langkah berikutnya adalah mengintegrasikan hasil *mangle* dengan aturan pada *Filter Rules*. Di sini, paket atau koneksi yang telah ditandai akan diblokir agar tidak diteruskan ke *client*. Hal ini memastikan bahwa pengguna dalam jaringan tidak dapat mengakses konten yang telah ditentukan sebagai terlarang. Proses

konfigurasi ini dilakukan menggunakan aplikasi WinBox agar pengelolaan perangkat RB750 menjadi lebih mudah dan cepat.

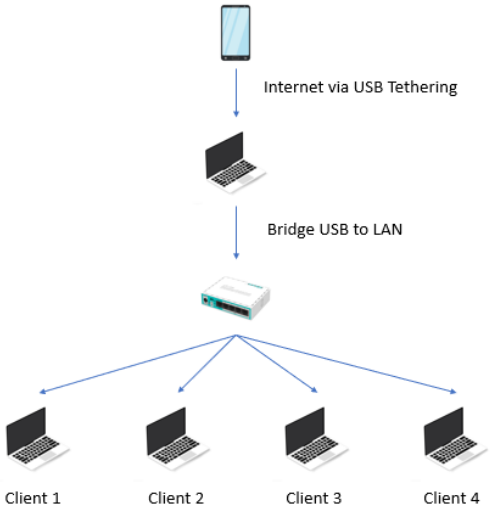
Pengujian dilakukan dengan mencoba mengakses situs-situs yang telah difilter menggunakan perangkat *client*. Jika filtering berhasil, maka situs tersebut tidak akan terbuka di browser. Selain itu, dilakukan juga pengamatan terhadap performa jaringan setelah implementasi filter, termasuk kestabilan koneksi, penggunaan CPU *router*, serta kecepatan akses situs yang tidak diblokir.

Melalui metode ini, peneliti dapat mengevaluasi seberapa efektif fitur *mangle* dalam membantu administrator jaringan untuk meningkatkan keamanan dan produktivitas jaringan lokal, dengan cara meminimalkan akses ke situs-situs yang tidak relevan atau berbahaya.

4. HASIL DAN PEMBAHASAN

Konfigurasi Jaringan

Topologi jaringan terdiri dari satu unit RB750 yang terhubung ke ISP dan satu perangkat *client*. Pengaturan dasar jaringan seperti IP *address*, NAT, dan DNS berhasil dilakukan tanpa kendala. *Router* memberikan koneksi internet ke *client* secara stabil sebelum filtering diterapkan.



Gambar 2. Topologi jaringan

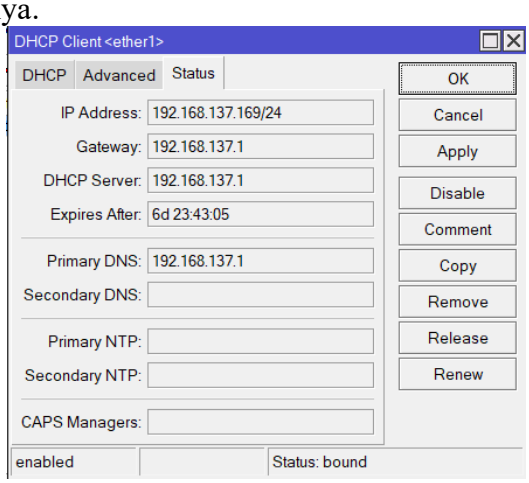
Langkah Penyambungan *Router* ke Jaringan Internet

Setelah koneksi internet berhasil diterima melalui laptop dari *tethering* HP via USB, langkah selanjutnya adalah menyambungkan koneksi tersebut ke *router* MikroTik RB750. Laptop yang telah menerima akses internet kemudian dihubungkan ke port ether1 pada *router* menggunakan kabel LAN. *Interface* ether1 pada MikroTik difungsikan sebagai jalur masuk (WAN) untuk menerima koneksi internet dari laptop.

Agar router dapat menerima IP dari laptop, maka perlu dilakukan konfigurasi DHCP *Client* pada *interface* ether1. Langkah-langkah konfigurasi tersebut adalah sebagai berikut:

1. Masuk ke menu IP → DHCP *Client* pada Winbox atau WebFig.
2. Tambahkan DHCP *Client* baru dan pilih *interface* ether1.
3. Klik Apply dan OK untuk mengaktifkan DHCP Client.

Setelah konfigurasi ini selesai, *router* MikroTik akan mendapatkan IP secara otomatis dari laptop dan dapat digunakan untuk meneruskan koneksi internet ke perangkat lain melalui port LAN lainnya.

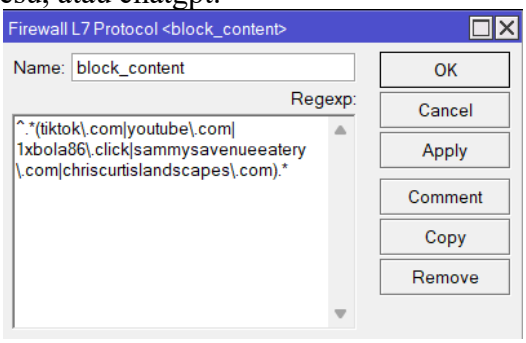


Gambar 3. Tampilan setting DHCP client

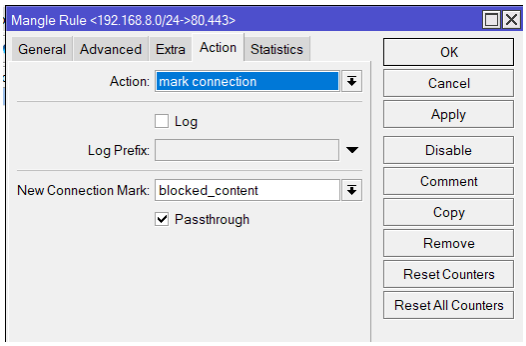
Implementasi *Mangle Filtering*

Penerapan *mangle rules* dilakukan untuk menandai lalu lintas berdasarkan konten menggunakan metode:

1. *Mark Connection*: untuk menandai koneksi yang mengarah ke domain tertentu.
2. *Mark Packet*: untuk menandai paket dari koneksi yang telah ditandai.
3. *Layer-7 Protocol Filtering*: untuk memblokir situs berdasarkan pola URL seperti youtube, otakudesu, atau chatgpt.



Gambar 4. Konfigurasi *content* yang ingin diblokir

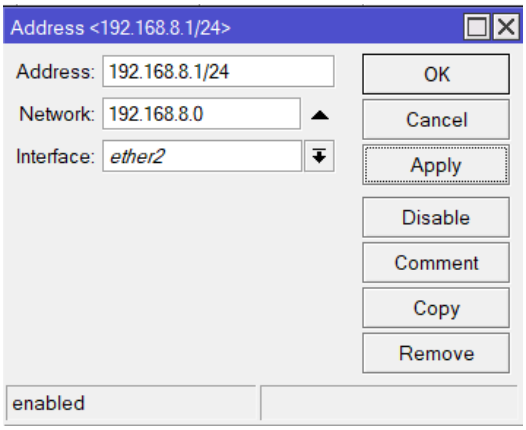


Gambar 5. Konfigurasi *mangle filtering content*

Pembuatan DHCP Server

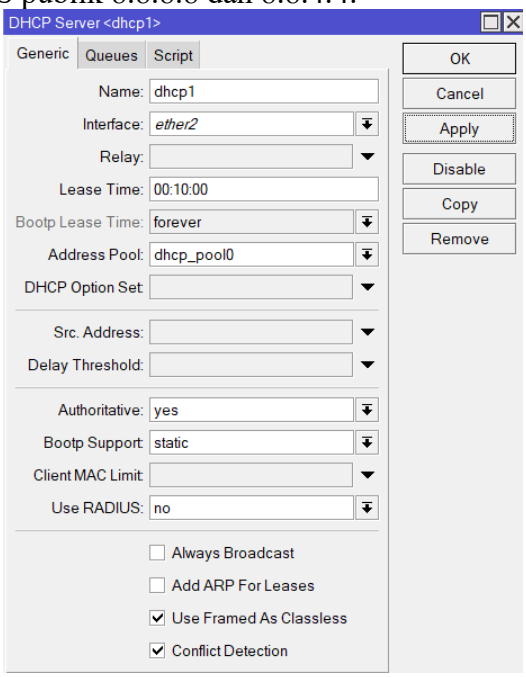
Agar *router* dapat mendistribusikan koneksi internet ke perangkat lain, maka perlu dibuat DHCP *Server* pada *interface* ether2, yang berfungsi sebagai jalur keluar koneksi atau LAN. Pertama-tama, *interface* ether2 perlu diberikan alamat IP statis sebagai identitas *gateway* jaringan lokal. Setelah itu, DHCP *Server* dikonfigurasi agar setiap perangkat yang terhubung secara otomatis mendapatkan alamat IP, *gateway*, dan DNS dari *router*.

Langkah awal yang dilakukan adalah mengatur IP *address* untuk *interface* ether2 pada *router*. Caranya, masuk ke menu IP → *Addresses*, lalu tambahkan IP *address* statis. Sebagai contoh, digunakan alamat 192.168.8.1/24 yang ditetapkan pada *interface* ether2. Alamat ini akan menjadi *gateway* bagi perangkat-perangkat yang terhubung melalui LAN.



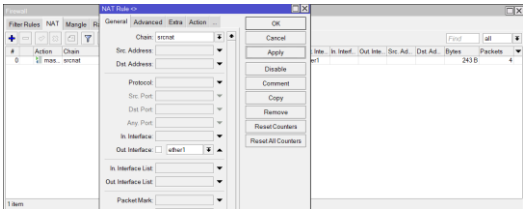
Gambar 6. Membuat alamat untuk client yang terhubung

Setelah itu, dibuat DHCP *Server* untuk memudahkan pembagian IP secara otomatis kepada perangkat *client*. Proses ini dilakukan melalui menu IP → DHCP *Server* → DHCP *Setup*, lalu memilih *interface* ether2. Dalam proses konfigurasi, diisikan beberapa parameter penting seperti rentang IP 192.168.8.2 - 192.168.10.254, *gateway* 192.168.10.1, serta DNS publik 8.8.8.8 dan 8.8.4.4.



Gambar 7. Konfigurasi DHCP server

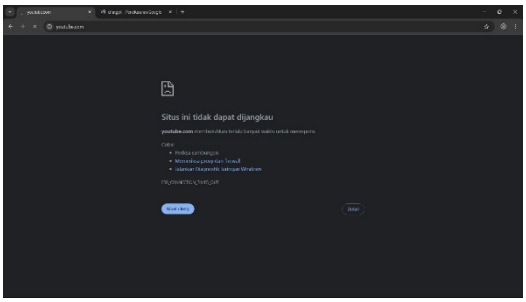
Agar perangkat yang mendapatkan IP dari *router* dapat mengakses internet, perlu ditambahkan aturan NAT. Masuk ke menu IP → *Firewall* dan buka tab NAT, kemudian buat *rule* baru dengan pengaturan *chain srcnat*, *out interface* ether1, dan *action masquerade.*



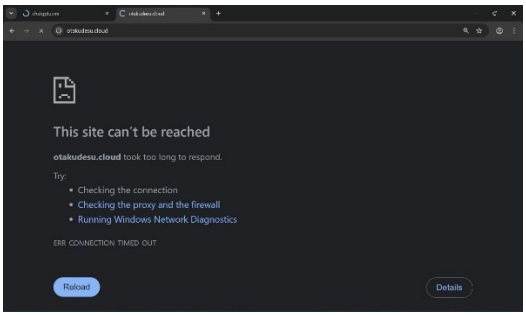
Gambar 8. Konfigurasi NAT

Hasil Percobaan

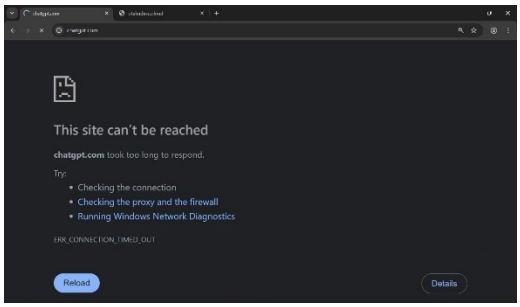
Percobaan dilakukan pada Google Chrome dan mengakses *keyword* YouTube, OtakuDesu dan ChatGPT yang sudah di *setting* agar tidak bisa mengakses jaringan internet.



Gambar 9. Laman youtube yang tidak bisa dibuka



Gambar 10. Laman otakudesu yang tidak bisa dibuka



Gambar 11. Laman chatgpt yang tidak bisa dibuka

Berdasarkan hasil percobaan yang telah dilakukan, implementasi metode *Mangle Filtering Content* pada perangkat MikroTik RB750 berhasil melakukan pemblokiran pada laman YouTube, OtakuDesu dan ChatGPT. Ini menandakan bahwa *filtering content* terbukti efektif dalam meningkatkan keamanan jaringan dengan cara memblokir akses terhadap situs-situs tertentu yang tergolong tidak diinginkan.

Pengaruh Terhadap Performa Jaringan

Penerapan metode dan konfigurasi jaringan memberikan pengaruh signifikan terhadap performa jaringan secara keseluruhan. Salah satu dampak utamanya adalah peningkatan efisiensi dalam pengiriman data, di mana konfigurasi yang tepat mampu mengurangi waktu tunda (*delay*) dan mempercepat proses transmisi paket. Selain itu, pengaturan jaringan yang baik juga berperan dalam mengurangi kemacetan (*congestion*) pada jalur komunikasi, terutama saat jaringan diakses oleh banyak pengguna secara bersamaan. Hal ini berdampak langsung pada kestabilan dan keandalan koneksi. Di sisi lain, kualitas layanan (*Quality of Service*/QoS) juga meningkat melalui pengelompokan dan prioritas trafik, yang memungkinkan layanan penting seperti video *streaming* atau VoIP berjalan lancar tanpa gangguan. Tak kalah penting, tingkat kehilangan paket (*packet loss*) dapat ditekan seminimal mungkin berkat desain jaringan dan pemilihan protokol yang sesuai, sehingga menjaga integritas dan keutuhan data yang dikirimkan. Secara keseluruhan, pengaruh-pengaruh tersebut juga memperkuat kemampuan jaringan untuk berkembang dan beradaptasi dengan kebutuhan yang terus meningkat, menjadikannya lebih skalabel dan andal di masa depan.

5. KESIMPULAN DAN SARAN

Penelitian ini membuktikan bahwa implementasi Mangle Filtering Content menggunakan MikroTik RB750 efektif dalam meningkatkan keamanan jaringan lokal, khususnya melalui fitur Layer-7 Protocol Filtering yang mampu memblokir akses ke situs tertentu seperti media sosial dan konten dewasa. Hasil uji coba menunjukkan sistem berhasil mencegah akses ke laman yang telah difilter, serta memberikan dampak positif terhadap performa jaringan seperti peningkatan stabilitas, efisiensi bandwidth, dan pengurangan delay. Untuk penelitian selanjutnya, disarankan agar fokus diarahkan pada pengujian performa jaringan menggunakan skenario beban yang lebih kompleks dan dinamis, serta membandingkan efektivitas berbagai protokol routing atau metode QoS yang berbeda. Penambahan aspek keamanan jaringan dan simulasi skalabilitas juga dapat menjadi arah penelitian berikutnya guna menghasilkan sistem jaringan yang lebih adaptif dan andal.

6. DAFTAR PUSTAKA

[1] L. N. Sukaryati and A. Voutama, "Penerapan metode Simple Additive Weighting pada sistem pendukung keputusan untuk memilih karyawan terbaik," *Jurnal Ilmiah MATRIK*, vol. 24, no. 3, pp. 260–267, 2022.

[2] W. A. Wiwi et al., "Sosialisasi Penggunaan Internet Yang Sehat Bagi Anak-Anak Di Yayasan Domyadhu," *Abdi Jurnal Publikasi*, vol. 1, no. 1, pp. 13–17, 2022.

[3] H. S. Nugraha, D. A. B. Assa, and I. Nisaa, "Rancang Bangun Kendali Pakan Ikan Lele Jarak Jauh Berbasis Internet Of Things (IoT)," *JTEKMEN*, vol. 1, no. 1, pp. 13–22, 2023.

[4] F. Nelfianti, R. Martiwi, A. Rahman, and A. Kurniawan, "Pelatihan Internet Sehat Dan Aman Untuk Remaja," *RESWARA: Jurnal Pengabdian Kepada Masyarakat*,

vol. 3, no. 1, pp. 115–122, 2022.
[5] W. Wiryanto, "Proses pembelajaran matematika di sekolah dasar di tengah pandemi covid-19," *Jurnal Review Pendidikan Dasar: Jurnal Kajian Pendidikan Dan Hasil Penelitian*, vol. 6, no. 2, pp. 125–132, 2020.
[6] M. F. Zulfi, O. Alvansyah, A. Y. Al-Hafiz, dan D. Kiswanto, "Pengujian Keamanan Jaringan Menggunakan Kali Linux di Lingkungan Google Cloud Platform," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 1, 2025.
[7] A. Syafiq, A. D. Putra, dan F. Asharudin, "Penerapan manajemen bandwidth dan filtering website menggunakan Layer 7 pada MikroTik di Tajir.net," *Jurnal Teknologi Informasi dan Komputer (JuTIK)*, vol. 9, no. 4, pp. 366–372, Jun. 2023.
[8] A. Maulana, N. Suharto, dan A. Hariyadi, "Implementation of MikroTik firewall for website access restriction and prevention of DoS (Denial of Service) attacks on internet networks of Al-Mahrusiyah Vocational School Lirboyo," *Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi)*, vol. 13, no. 1, pp. 81–86, 2023.
[9] Y. K. Putra, M. Sadali, dan Mahpuz, "Penerapan Mikrotik dalam mengembangkan infrastruktur jaringan pada Kantor Desa Rumbuk Kecamatan Sakra," *Infotek: Jurnal Informatika dan Teknologi*, vol. 3, no. 2, pp. 182–193, Jul. 2020.
[10] R. S. Budi dan I. Sembiring, "Implementasi keamanan jaringan komputer dengan iptables sebagai firewall menggunakan port knocking metode dinamis," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 10, no. 1, pp. 720–738, Mar. 2025.
[11] W. D. Putra dan Munaldi, "Perancangan dan simulasi jaringan komputer dengan keamanan firewall," *JRIIN: Jurnal Riset Informatika dan Inovasi*, vol. 2, no. 9, pp. 1761–1767, Feb. 2025.
[12] Munira, Dasril, dan H. Abduh, "Membangun web filtering dengan DNS forwarding pada jaringan wireless berbasis Mikrotik pada SMA Negeri 1 Palopo," *Jurnal Riset Sistem Informasi*, vol. 1, no. 3, pp. 37–44, Jul. 2024.
[13] Muklas, H. Supendar, dan S. SW, "Optimalisasi sistem keamanan jaringan komputer menggunakan metode filtering dan manajemen bandwidth pada PT. Intav Prima Solusindo," *TEKINFO*, vol. 21, no. 1, pp. 104–111, Apr. 2020.
[14] H. P. Fitrian, F. Dani, I. Fadilah, R. D. Fauzan, dan M. R. Ardhyansyah, "Implementasi Mikrotik firewall sebagai solusi filtering situs judi online dalam jaringan," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 1, pp. 1685–1691, Feb. 2025.
[15] S. Hamza, "Pemanfaatan firewall mangle untuk pengaturan packet data menggunakan mark connection, mark packet, dan mark routing dengan RouterBoard RB941-2nD," *Jurnal BIOSAINSTEK*, vol. 4, no. 2, pp. 27–33, Jul. 2022.
[16] M. Noviansyah, "Efisiensi jaringan komputer dengan penerapan firewall mangle dan bandwidth limit dengan metode Per Connection Queuing (PCQ)," *Jurnal AKRAB Juara*, vol. 8, no. 1, pp. 116–124, Feb. 2023.