Computer Science (CO-SCIENCE)
Vol. 5 No. 2 Juli 2025
Akreditasi Sinta 4 Nomor SK : 230/E/KPT/2022

Implementasi Firewall Mikrotik dalam Pembatasan Akses Situs Terlarang di RT/RW Net

Hanggoro Aji Al Kautsar[1*], Ricki Sastra[2]

[1]Program Studi Informatika, Fakultas Teknik dan Informatika, Universitas Bina Sarana Informatika
Jl. Kramat Raya No. 98 Senen, Jakarta Pusat - 10420, Indonesia

[2]Program Studi Rekayasa Perangakat Lunak, Fakultas Teknik dan Informatika, Universitas Bina Sarana Informatika Jl. Kramat Raya No. 98 Senen, Jakarta Pusat - 10420, Indonesia

e-mail: [1]hanggoro.hgr@bsi.ac.id, [2]ricki.rkt@bsi.ac.id

(*) Corresponding Author

Artikel Info : Diterima : 16-05-2025 | Direvisi : 25-06-2025 | Disetujui : 23-07-2025

Abstrak - Penggunaan internet yang semakin meluas di lingkungan RT/RW Net membawa dampak positif dan negatif. Salah satu permasalahan yang muncul adalah akses bebas terhadap konten yang tidak sesuai untuk kalangan pelajar, seperti game online, situs pornografi, dan judi online. Penulisan ini bertujuan untuk membatasi hak akses pengguna internet di jaringan RT/RW Net dengan menerapkan firewall filter pada router MikroTik. Metode yang digunakan adalah konfigurasi *firewall filtering* berdasarkan IP, *port, domain, layer 7, Mangle Rule*, dan yang lainnya. Hasil penulisan menunjukkan bahwa penerapan firewall filter pada router MikroTik dengan mengunakan aplikasi Winbox mampu membatasi akses terhadap situs-situs yang dilarang secara efektif dan meningkatkan keamanan jaringan. Uji coba dilakukan sebelum dan sesudah konfigurasi, dengan hasil menunjukkan keberhasilan pemblokiran konten yang tidak diinginkan.

Kata Kunci : *Firewall*, RT/RW Net, *Filtering,* Mikrotik

Abstracts *- The increasing use of the Internet in RT/RW Net environments has brought both positive and negative impacts. One issue is the unrestricted access to inappropriate content, especially among students, such as online games, pornography, and gambling websites. This study aims to restrict internet user access rights in RT/RW Net networks by implementing firewall filters on MikroTik routers. The method used is firewall filtering configuration based on IP, port, and domain restrictions. The results show that the implementation of the firewall filter on MikroTik routers effectively blocks access to restricted sites and improves network security. Tests were carried out before and after configuration, showing the successful blocking of unwanted content. standards.*

Keywords : Firewall, RT/RW Net, *Filtering, Mikrotik*

PENDAHULUAN

Perkembangan teknologi internet telah membawa dampak signifikan dalam berbagai aspek kehidupan, termasuk pendidikan. Internet menyediakan banyak kemudahan kepada kita di berbagai bidang. Salah satunya adalah dalam bidang pendidikan dan hiburan (Purwianti et al., 2022). Namun, di sisi lain, kemudahan akses internet juga membuka peluang bagi pengguna, terutama pelajar, untuk mengakses konten-konten negatif yang dapat merugikan perkembangan mereka. Konten seperti game online yang berlebihan, situs pornografi, dan situs judi online dapat mengganggu konsentrasi belajar, menurunkan prestasi akademik, dan bahkan berdampak buruk pada kesehatan mental dan sosial. Perkembangan teknologi informasi begitu penting dan diterima dengan baik oleh masyarakat sebab berperan sebagai sarana efektif untuk mengatasi berbagai kendala di berbagai sektor. (Sukaryati et al., 2022)

Jaringan RT/RW Net, sebagai salah satu solusi akses internet yang terjangkau di lingkungan masyarakat, memiliki peran penting dalam menyediakan konektivitas. Namun, seringkali pengelolaan keamanan dan pembatasan akses pada jaringan ini masih minim. Akibatnya, pengguna, termasuk pelajar, memiliki kebebasan akses yang tidak terkontrol terhadap berbagai jenis konten di internet.

Betapa krusialnya akses internet di era sekarang. Dari berkirim email, mencari berita, berselancar di media sosial, bertransaksi perbankan, berbelanja online, hingga chatting dan mengakses aplikasi daring, semua membutuhkan internet (Cholik, 2021). Sayangnya, di balik manfaat positifnya, internet juga menyimpan banyak potensi negatif (Walidaini et al., 2018).

Penerapan sistem keamanan jaringan sangat dibutuhkan dalam membatasi akses terhadap konten negatif tersebut. Salah satu solusi efektif adalah dengan menggunakan *firewall filtering* yang tersedia pada perangkat router MikroTik. MikroTik menyediakan fitur filtering yang memungkinkan administrator jaringan memblokir akses berdasarkan IP address, domain, dan port tertentu. Penulisan ini bertujuan untuk menerapkan metode *firewall filter* dalam membatasi hak akses internet pengguna jaringan RT/RW Net dengan fokus pada filtering konten yang tidak sesuai bagi pelajar. Berbagai platform daring seperti internet, media sosial, iklan, game, film, dan klip video berpotensi menjadi jalan bagi anak-anak untuk terpapar konten pornografi. Paparan tersebut, disengaja atau tidak, dapat membangkitkan rasa ingin tahu yang mendorong mereka untuk menjelajahi lebih banyak konten serupa (Lase & Halawa, 2022). Salah satu solusi untuk mengatasi permasalahan ini adalah dengan mengimplementasikan *firewall filter* pada perangkat router yang digunakan dalam jaringan RT/RW Net. Web filtering adalah teknik yang digunakan untuk membatasi akses pengguna ke konten tertentu di internet. Menurut (Syarief & Bardul, 2023) intinya, penyaringan web atau *web filtering* adalah mekanisme untuk mengendalikan situs web mana yang boleh dan tidak boleh diakses oleh pengguna. Ini diterapkan untuk mencegah akses ke konten yang tidak pantas, serta untuk mengoptimalkan keamanan, produktivitas, dan kepatuhan dalam penggunaan jaringan..

Untuk memblokir akses web, MikroTik menyediakan beragam cara seperti static DNS, content filter, web proxy, route policy, firewall Layer 7, atau pemblokiran alamat IP/port. Dalam konteks penulisan ini, pemblokiran dilakukan menggunakan protokol Layer 7. Metode ini berfungsi dengan mencari pola dalam paket data yang bergerak melalui ICMP, TCP, dan UDP. Penting dicatat bahwa Firewall Layer 7 pada MikroTik jauh lebih canggih dan kompleks dibandingkan dengan jenis firewall lainnya (Syafiq et al., 2023). Firewall filter bekerja dengan cara memeriksa lalu lintas jaringan berdasarkan aturan-aturan yang telah ditentukan, sehingga memungkinkan administrator jaringan untuk memblokir atau mengizinkan akses ke alamat IP, port, protokol, atau bahkan konten tertentu. Dalam rancangan ini, penulis menerapkan manajemen keamanan internet melalui *filter firewall* berbasis konten. Tujuannya adalah membatasi akses ke situs media sosial, web dengan konten negatif, dan pornografi yang sama sekali tidak berhubungan dengan aktivitas pekerjaan. (Riyana Rahadjeng & Ihsan Fajrin, 2021).

Sebagai perangkat keras, router didesain untuk menerima, menganalisis, dan memindahkan paket data dari satu jaringan ke jaringan lainnya. Fungsinya juga mencakup konversi paket untuk antarmuka jaringan yang beragam, pemblokiran akses, dan berbagai tindakan lain terkait pengelolaan jaringan (Ali & Latifah, 2021) Router Mikrotik merupakan salah satu perangkat jaringan yang populer digunakan dalam implementasi RT/RW Net karena fitur-fiturnya yang lengkap dan fleksibilitas konfigurasinya, termasuk kemampuan firewall filtering yang mumpuni. Dengan konfigurasi yang tepat, firewall pada router Mikrotik dapat menjadi solusi efektif dalam membatasi hak akses pengguna terhadap konten-konten negatif. Mikrotik adalah salah satu perangkat jaringan yang banyak digunakan untuk manajemen bandwidth dan web filtering. Menurut (Imansyah et al., 2021) Sebagai penyedia hardware dan software untuk router, MikroTik menawarkan MikroTik RouterOS, sebuah sistem operasi yang diinstal pada komputer untuk menjadikannya router. RouterOS ini kaya akan fitur dan tools yang dibutuhkan untuk membangun router yang kuat dan stabil. Oleh karena itu, penerapan filter Layer 7 protokol bisa meningkatkan efisiensi waktu kerja jaringan. Ditambah lagi, adanya fitur hotspot pada router MikroTik akan memudahkan administrator dalam mengawasi penggunaan jaringan oleh karyawan di perusahaan (Ali & Latifah, 2021) Menurut (Sari, 2024) *Application layers* adalah lapisan yang menjadi pusat interaksi antara pengguna dengan aplikasi yang bekerja dengan fungsi sebuah jaringan. Fungsi lainnya adalah melakukan konfigurasi mengenai cara aplikasi bekerja menggunakan sumber daya jaringan. Sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan – pesan kesalahan. Apabila terjadi kesalahan pada proses pengaturan jaringan lapisan ini, maka lapisan bisa memberikan pesan. Contoh services dan protocol yang berlaku seperti HTTP, SMTP, FTP, NFS dan ada beberapa lainnya.

Web filtering adalah teknik yang digunakan untuk membatasi akses pengguna ke konten tertentu di internet. Menurut (Wuhi et al., 2024) secara sederhana, filter web adalah proses pengaturan akses pengguna ke situs web. Ini dilakukan untuk menghalangi atau membatasi kunjungan ke situs yang dianggap tidak sesuai, serta untuk memperbaiki keamanan, produktivitas, dan kepatuhan di lingkungan jaringan. Menurut (Yunif Lukman Hakim & HendroWijayanto, 2024) *Layer 7 Protocol*, atau juga dikenal sebagai lapisan aplikasi, bertindak sebagai jembatan antara aplikasi dan fungsi jaringan. Ini mengatur cara aplikasi berinteraksi dengan jaringan dan bertanggung jawab untuk menghasilkan pesan kesalahan. Protokol umum yang termasuk dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS. Selain itu, Layer 7 Protocol juga memiliki kemampuan untuk memblokir situs web dengan menambahkan aturan filter baru.

Pada perancangan kali ini, kami menggunakan software winbox dan metode MRTG untuk melakukan konfigurasi pada router. Winbox merupakan sebuah utilitas yang memungkinkan pengguna untuk melakukan remote terhadap server MikroTik melalui antarmuka grafis (GUI). Menurut (Sugandi et al., 2023) Winbox adalah alat yang kuat dan efisien untuk mengelola perangkat MikroTik dengan antarmuka grafis yang intuitif, memudahkan pengguna dalam melakukan berbagai pengaturan dan konfigurasi jaringan. Sedangkan menurut (Gaffar, 2021) *Multi Router Traffic Grapher* adalah tool yang biasa digunakan untuk memonitor beban trafik (traffic load) dalam suatu jaringan pada kurun waktu tertentu dalam bentuk tampilan grafis. Keunggulan dari MRTG adalah faktor kesederhanaan dan fungsionalitasnya. MRTG dapat dikonfigurasi dengan mudah untuk memantau penggunaan bandwitdh dalam suatu perangkat yang mendukung SNMP, yang dapat memantau trafik

dalam jangka waktu yang diinginkan user.

Penulisan ini bertujuan untuk mengimplementasikan dan menguji efektivitas firewall filter pada router Mikrotik dalam membatasi hak akses internet di lingkungan jaringan RT/RW Net, dengan fokus pada pemblokiran akses ke game online, situs pornografi, dan situs judi online yang sering diakses oleh pelajar. Diharapkan hasil penulisan ini dapat memberikan kontribusi praktis dalam meningkatkan keamanan dan menciptakan lingkungan internet yang lebih sehat bagi pengguna jaringan RT/RW Net.

METODE PENULISAN

Metode penulisan mencakup seluruh proses pengumpulan data, analisis, dan interpretasi yang relevan dengan tujuan penulisan. Dalam upaya pengembangan sistem ini, penulis memilih untuk menggunakan model NDLC (Network Development Life Cycle). Model ini terdiri dari enam fase krusial: analisis, desain, simulasi, monitoring, implementasi, dan manajemen.
Dan teknik pengumpulan data yang penulis lakukan pada penilitian ini adalah :

1. Observasi
   Tujuan dari proses ini adalah untuk mendapatkan pemahaman, analisis, atau pemahaman yang akurat tentang objek atau situasi yang diamati. Penulis menggunakan metode ini agar merasakan langsung bagaimana kinerja jaringan komputer digunakan dan dimengerti oleh pengguna terkait kualitasnya.
2. Studi Pustaka
   Metode untuk mengumpulkan data atau informasi dengan membaca berbagai sumber tertulis yang berkaitan dengan topik yang sedang diteliti. Mengkaji referensi terkait sistem keamanan jaringan, firewall filtering, dan konfigurasi MikroTik. Kami juga melakukan penelusuran literatur terkait konsep firewall, firewall filtering, router Mikrotik, keamanan jaringan, dan isu-isu terkait dampak negatif internet pada pelajar

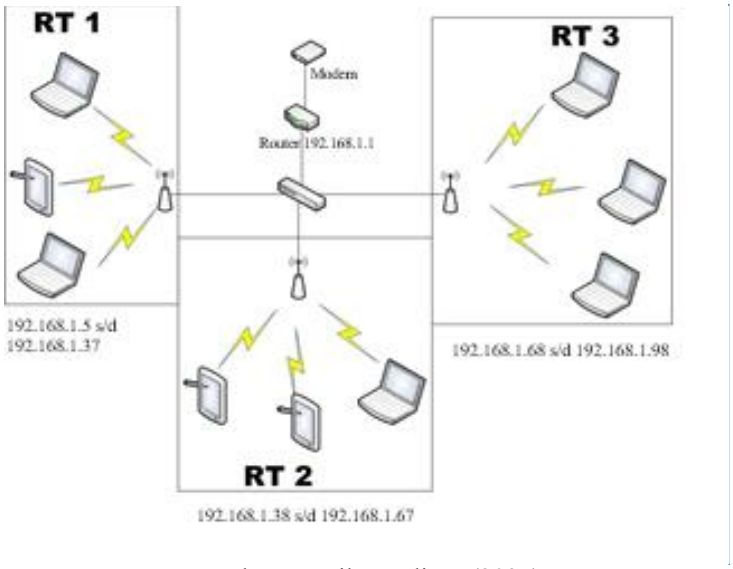
Tahapan Penulisan

Penulisan ini menggunakan metode studi kasus dengan pendekatan eksperimental. Langkah-langkah penulisan yang dilakukan adalah sebagai berikut:

1. Studi Literatur
   Melakukan penelusuran literatur terkait konsep firewall, firewall filtering, router Mikrotik, keamanan jaringan, dan isu-isu terkait dampak negatif internet pada pelajar.
2. Perancangan Skema Jaringan
   Menggambarkan topologi jaringan RT/RW Net yang menjadi studi kasus, termasuk perangkat router Mikrotik yang digunakan.
3. Perancangan Sistem Keamanan Jaringan
   Merencanakan implementasi firewall filter pada router Mikrotik untuk membatasi akses ke kategori konten yang telah ditentukan (game online, situs pornografi, situs judi online).
4. Konfigurasi Firewall Filtering
   Menerapkan konfigurasi firewall filter pada router Mikrotik sesuai dengan rancangan yang telah dibuat. Konfigurasi ini meliputi pembuatan rule firewall yang memblokir akses ke alamat IP atau domain yang relevan dengan kategori konten yang ditargetkan.
5. Pengujian Awal
   Melakukan pengujian awal setelah konfigurasi firewall diterapkan untuk memastikan bahwa rule firewall berfungsi sesuai dengan yang diharapkan dan tidak menghambat akses ke situs atau layanan yang seharusnya diizinkan.
6. Pengujian Akhir
   Melakukan pengujian akhir dengan melibatkan beberapa pengguna (simulasi pelajar) untuk menguji efektivitas firewall dalam memblokir akses ke situs dan aplikasi yang ditargetkan. Pengujian ini mencakup upaya mengakses situs game online populer, situs pornografi, dan situs judi online melalui perangkat yang terhubung ke jaringan RT/RW Net.
7. Analisis Hasil
   Menganalisis data hasil pengujian untuk mengevaluasi efektivitas implementasi firewall filter dalam membatasi hak akses. Data yang dianalisis meliputi keberhasilan pemblokiran akses dan potensi dampak terhadap pengalaman pengguna.
8. Evaluasi
   Tahapan ini merupakan tahapan setelah proses pengujian sistem sudah dilakukan. Hasil dari tahapan evaluasi dijadikan dasar apakah manajemen keamanan internet berbasis penyaringan konten (content filtering) dinyatakan berhasil dan efektif atau tidak.

HASIL DAN PEMBAHASAN

Skema Jaringan



Sumber : Hasil Penulisan (2025)
Gambar 1. Skema Jaringan

Skema adalah sebuah struktur dari sebuah jaringan komputer.Skema akan menggambarkan jaringan secara keseluruhan darei jaringan komputer yang ada. Pada jaringan RT/RW net yg kami racang ini menggunakan topologi Star. Hal ini menyangkut fungsi dan efisiensi dalam penyimpanan dan pengolahan data sehingga dapat terkontrol dengan baik dan lancar. Pada jaringan internet ini distribusi sumber informasi menggunakan jaringan terdistribusi dengan topologi star. Skema jaringan meliputi Router yang berfungsi menghubungkan Internet dengan jaringan lokal perusahaan. Bagi perangkat wired (menggunakan kabel) terhubung terlebih dahulu ke switch, melalui port port LAN yang tersedia disetiap meja dan switch disini berfungsi sebagai penghubung perangkat wired dengan server dan bagi pengguna wireless.

Tabel 1. Pembagian IP Address

Lokasi	Perangkat Keras	IP Address
Master	Router RB750 Modem Switch (VLAN)	192.168.1.1
RT 1	Client 1 (30 client)	192.168.1.5 s/d 192.168.1.37
RT 2	Client 2 (30 client)	192.168.1.38 s/d 192.168.1.67
RT 3	Client 3 (30 client)	192.168.1.68 s/d 192.168.1.98

Sumber : Hasil Penulisan (2025)

Penjelasan IP Address yang digunakan pada jaringan RT/RW Net adalah IP address yang digunakan 192.168.1.0 dengan subneting 255.255.255.224. Pada dasarnya IP Address yang digunakan adalah termasuk ke dalam kelas C dengan IP Address dimuali dari 192.168.1.2 – 192.168.1.93 dan subnet mask default 255.255.255.224.

Rancangan Infrastruktur Jaringan

Penulis merancang infrastruktur jaringan dengan memanfaatkan beberapa aplikasi yang bertujuan meningkatkan kinerja jaringan dan mengelola konfigurasi akses internet, yang semuanya disimulasikan.. Berikut ini adalah aplikasi yang penulis gunakan :

1. Router MikroTik RB750
2. Laptop/PC
3. Winbox (aplikasi konfigurasi MikroTik)
4. Daftar situs dan port yang diblokir

Rancangan Sistem Keamanan Jaringan

Sistem keamanan jaringan yang diimplementasikan dalam penulisan ini berfokus pada penggunaan fitur firewall filter pada router Mikrotik. Firewall filter bekerja pada layer 3 dan 4 dari model OSI, memungkinkan administrator

untuk mengontrol lalu lintas jaringan berdasarkan alamat IP sumber dan tujuan, port, dan protokol.

Rancangan Firewall Filtering

Rancangan firewall filtering dalam penulisan ini bertujuan untuk memblokir akses ke kategori konten berikut:

1. Game Online
   Pemblokiran dilakukan berdasarkan alamat IP server game online populer dan/atau port yang umum digunakan oleh aplikasi game online.
2. Situs Pornografi
   Pemblokiran dilakukan berdasarkan daftar domain dan alamat IP situs-situs pornografi yang telah dikumpulkan melalui sumber-sumber terpercaya.
3. Situs Judi Online
   Pemblokiran dilakukan berdasarkan daftar domain dan alamat IP situs-situs judi online yang telah diidentifikasi.

Konfigurasi Firewall CLI

Pada konfigurasi ini, penulis menggunakan aplikasi Winbox untuk melakukan konfigurasi di router mikrotik. Adapun alur kerjanya adalah dengan menginventarisir alamt web yang akan di blokir, kemudian mendaftarkannya ke router untuk kemudian dilakukan pemblokiran web tersebut. Adapun untuk pemblokiran web yang penulis lakukan pada kesempatan kali ini adalah memblok situs belanja tiket online. Hal ini dikarenakan situs-situs yang akan diblokir sebenarnya tidak mungkin untuk ditampilkan pada jurnal ini. Dan skenario yg penulis harapkan adalah sebagai berikut :

Tabel 2. Alamat web yang di blok

URL	Sebelum *filtering*	Sesudah *filtering*
https://www.tiket.com/	*Allow*	*Drop/Deny*
https://shopee.co.id/	*Allow*	*Drop/Deny*
https://tokopedia.com/	*Allow*	*Drop/Deny*
https://www.blibli.com/	*Allow*	*Drop/Deny*

Sumber : Hasil Penulisan (2025)

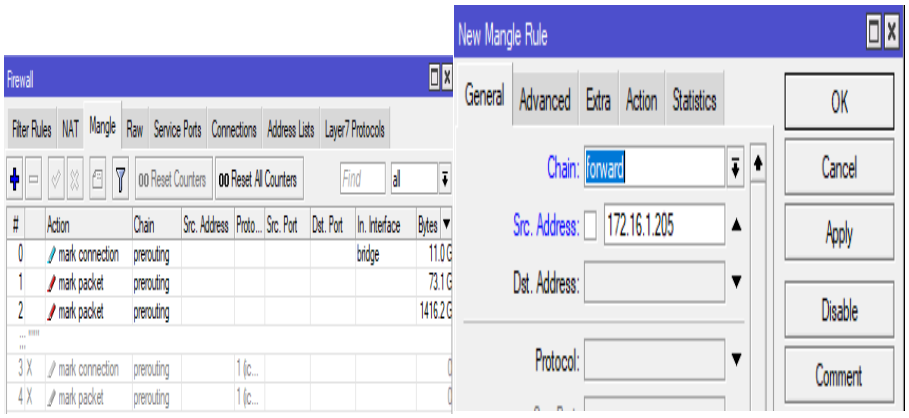
Konfigurasi firewall filter pada router Mikrotik dilakukan melalui antarmuka command-line (CLI) atau graphical user interface (GUI) Winbox. Berikut ini adalah listing untuk CLI :

```
/ip firewall filter
add action=drop chain=forward dst-port=443 protocol=tcp comment="Blokir Game Online (TCP)"
add action=drop chain=forward dst-port=443 protocol=udp comment="Blokir Game Online (UDP)"
add action=drop chain=forward dst-address-list=pornography_sites comment="Blokir Situs Pornografi"
add action=drop chain=forward dst-address-list=judi_online_sites comment="Blokir Situs Judi Online"
add chain=forward protocol=tcp port=6881-6999 action=drop comment="Blokir torrent"
```

Konfigurasi *mangle* diperlukan untuk membuat rule (aturan) untuk menandai paket data pada konfigurasi yang akan diterapkan. Disini penulis membuat dua rule mangle diantaranya untuk konfigurasi *mark connection* dan *mark packet*.

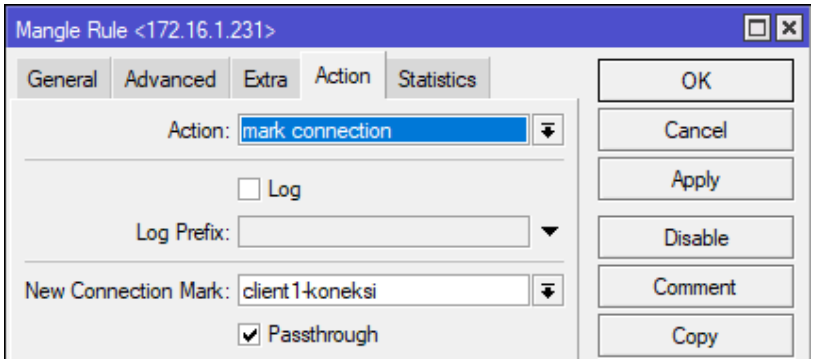
1. Membuat *rule mangle mark connection*

Untuk membuat rule mangle mark connection pergi ke IP-firewall-tab mangle. Pada gambar 2. klik logo “tambah biru” pada bagian kiri atas untuk menambah mangle rule.



Sumber : Hasil Penulisan (2025)
Gambar 2. *Rule Mangle*

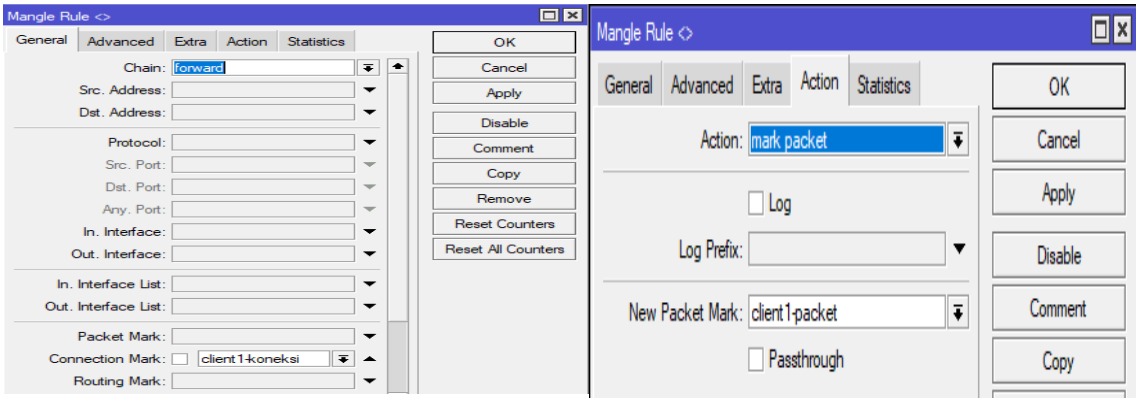
Pertama membuat rule pembatasan upload. Pada gambar di atas Chain disini untuk menetukan jenis trafik yang akan di-manage diisi dengan forward karena digunakan untuk memproses trafik paket data yang hanya melewati Router. Src.Address diisi IP address client yang ingin dilimit.



Sumber : Hasil Penulisan (2025)
Gambar 3. Konfigurasi *Action*

Selanjutnya ke tab action. Pada gambar diatas tab Action diisi mark connection untuk membuat paket baru, dan new connection mark diisi client1-koneksi. Beri centang pada passthrought untuk meneruskan ke rule dibawahnya. Setelah itu klik apply.

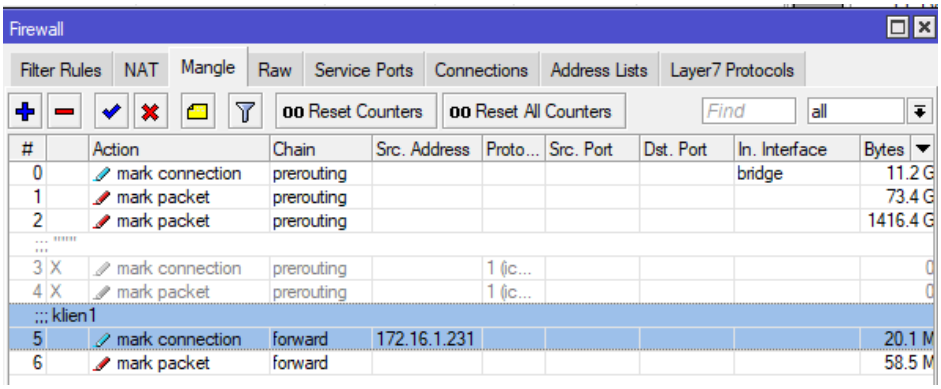
2. Membuat *rule mangle mark packet*



Sumber : Hasil Penulisan (2025)
Gambar 4. *Mangle Mark Packet*

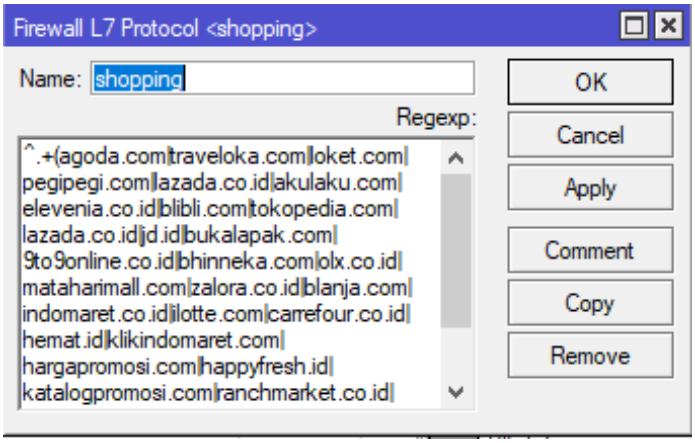
Sama seperti membuat rule mark connection klik logo “tambah biru” pada chain diisikan forward,pada connection mark dipilih paket yang sudah dibuat sebelumnya, lalu ke tab action. Pada tab Action diisi mark packet untuk

menandai paket yang ditentukan, dan pada new packet mark diisi client1-packet, ini yang akan di masukan pada queue tree nanti. Beri hilangkan centang pada passthrought. Setelah itu klik apply. Berikut ini tampilan sesudah ditambahkan mark-connection dan mark- packet.



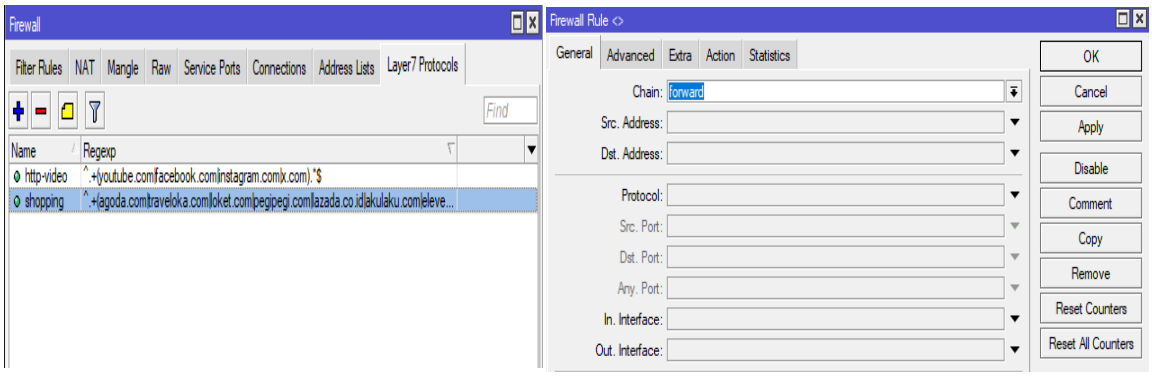
Sumber : Hasil Penulisan (2025)
Gambar 5. Hasil konfigurasi *Mangle Rule*

3. Konfigurasi Blocking Situs



Sumber : Hasil Penulisan (2025)
Gambar 6. Konfigurasi *Firewall layer 7*

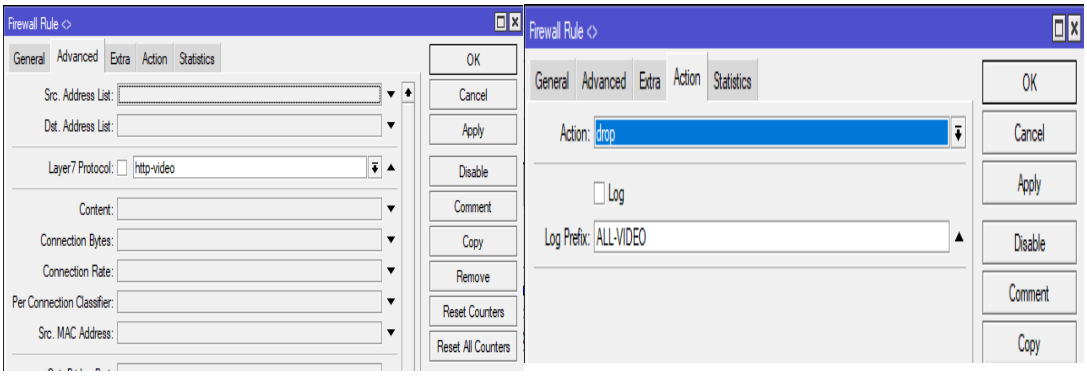
Konfigurasi blocking situs menggunakan dua tahap meliputi konfigurasi rule protocol layer7 dan diijinkan tidaknya (drop) untuk mengakses sebuah situs dikonfigurasi di dalam filter rule. Konfigurasi layer7 protocol diperlukan untuk membuat rule situs apa saja yang tidak boleh diakses, penulis memasukan situs belanja online seperti tokopedia, agoda, traveloka, loket dan lazada untuk tidak dapat diakses.



Sumber : Hasil Penulisan (2025)
Gambar 7. Pengaturan *Firewall Rule*

Masuk kedalam menu IP – firewall – masuk ke tab layer7 protocol, lalu tambah. Pada gambar 7 penulis membuat rule yang diberi name “shopping” untuk penamaan dan memasukan kode “^.+(situs yang akan di block).*$”. Konfigurasi Filter rules diperlukan untuk pemberi akses paket data. Masih di menu firewall, dibagian tab filter rule

lalu tambah. Pada gambar 8 chain yang merupakan jenis trafik diisi “forward” dikarnakan pengaturan untuk trafik data yang melalui Router. Selanjutnya pindah ke tab Advance. Pada tab Advance, dibagian layer7 protocol diisi rule yang telah dibuat tadi di konfigurasi layer7 protocol. Selanjutnya ke tab Action. Pada gambar diatas action diisi drop yang artinya akses untuk menuju ke layer7 protocol yang berisikan rule situs yang telah dibuat akan di block.



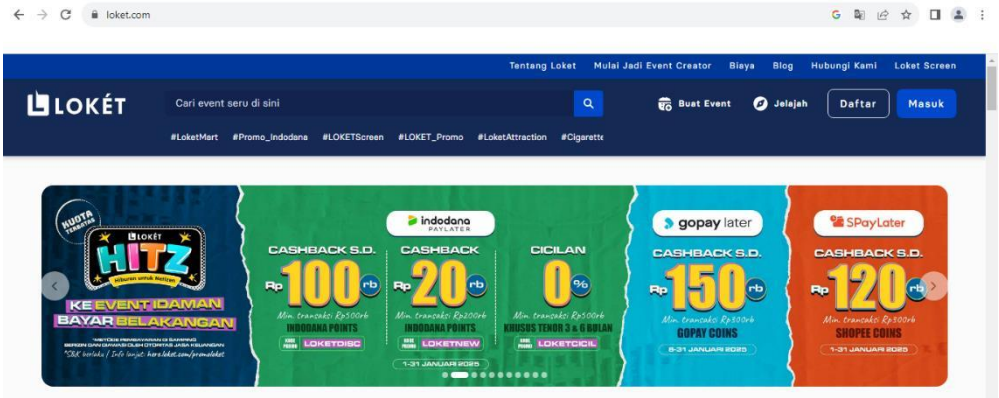
Sumber : Hasil Penulisan (2025)
Gambar 8. Konfigurasi *Firewall Rule drop*

Pengujian Jaringan

Pengujian jaringan komputer merupakan gambaran tentang rancangan jaringan komputer sebelum dan sesudahnya dilakukan konfigurasi pada jaringan tersebut. Ada dua tahap pengujian yang dilakukan diantaranya pengujian jaringan awal yaitu gambaran dilakukannya sebelum konfigurasi dilakukan dan pengujian tahap akhir yaitu gambaran dilakukan nya setelah konfigurasi dilakukan.

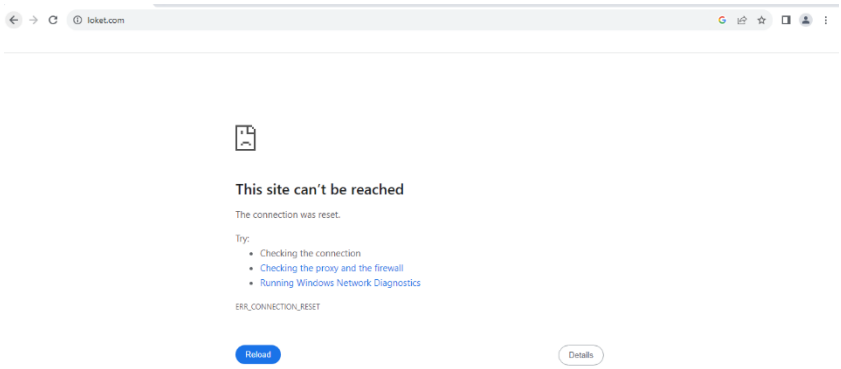
Pengujian Awal

Setelah konfigurasi *firewall* diterapkan, dilakukan pengujian awal untuk memastikan bahwa *rule firewall* bekerja sesuai dengan yang diharapkan. Pengujian ini melibatkan upaya mengakses situs-situs yang seharusnya diblokir dari perangkat yang terhubung ke jaringan. Hasil pengujian awal menunjukkan bahwa akses ke alamat IP dan port yang telah dikonfigurasi untuk pemblokiran berhasil ditolak oleh firewall. Selain itu, pengujian juga dilakukan untuk memastikan bahwa akses ke situs-situs dan layanan internet yang tidak termasuk dalam kategori yang diblokir tetap berjalan normal.



Sumber : Hasil Penulisan (2025)
Gambar 9. Tampilan awal web loket.com

Pengujian Akhir



Sumber : Hasil Penulisan (2025)
Gambar 10. Pengujian akhir web loket.com

Pengujian akhir melibatkan beberapa pengguna simulasi (pelajar) yang mencoba mengakses kategori konten yang telah ditentukan untuk diblokir. Namun dalam pengujian ini, penulis memblok situs belanja tiket online. Hal ini dikarenakan situs-situs yang akan diblokir sebenarnya tidak mungkin untuk ditampilkan pada jurnal ini. Hasil tampilannya seperti tampilan pada gambar 10 di atas. Dan hasil pengujian akhir menunjukkan bahwa implementasi firewall filter pada router Mikrotik terbukti efektif 100% dalam membatasi akses ke konten-konten negatif yang ditargetkan. Namun ketika penulis menggunakan aplikasi VPN, alamat web dapat terbuka kembali. Hal ini menunjukan adanya kelemahan dari metode firewall filtering.

KESIMPULAN

Berdasarkan hasil penulisan dan pembahasan, dapat disimpulkan bahwa implementasi firewall filter pada router Mikrotik efektif dalam membatasi akses internet di jaringan RT/RW Net, khususnya dalam memblokir akses ke game online, situs pornografi, dan situs judi online. Konfigurasi rule firewall yang tepat berdasarkan alamat IP dan domain terbukti 100% mampu mencegah pengguna mengakses konten-konten negatif tersebut. Selain itu penggunaan aplikasi Winbox pada perangkat Router MikroTik juga mudah di konfigurasi dan di implementasikan.

Penulisan selanjutnya dapat fokus pada metode pemblokiran yang lebih canggih untuk mengatasi upaya *bypassing* seperti penggunaan VPN, serta evaluasi dampak implementasi firewall terhadap pengalaman pengguna dan kinerja jaringan secara keseluruhan.

REFERENSI

Ali, M., & Latifah, F. (2021). IMPLEMENASI BLOCK ACCESS PENGGUNA LAYANAN INTERNET DENGAN METODE FILTER RULE dan LAYER 7 PROTOCOL. *Journal of Information System, Applied, Management, Accounting and Research*, *5*(2), 340–349. https://doi.org/10.52362/JISAMAR.V5I2.422

Cholik, C. A. (2021). Perkembangan Teknologi Informasi Komunikasi / ICT dalam Berbagai Bidang. *Jurnal Fakultas Teknik UNISA Kuningan*, *2*(2), 39–46.

Gaffar, A. W. M. (2021). Pengklasifikasian Kecepatan Transfer Data Pada Jaringan Backbone Menggunakan K-Means. *Buletin Sistem Informasi Dan Teknologi Islam (BUSITI); Vol 2, No 2 (2021)DO - 10.33096/Busiti.V2i2.982* . https://jurnal.fikom.umi.ac.id/index.php/BUSITI/article/view/982

Imansyah, F., Marpaung, J., Teknik Elektro, J., Teknik, F., & Tanjungpura Jln Hadari Nawawi, U. H. (2021). PENERAPAN METODE QUEUE TREE PADA BANDWIDTH MANAGEMENT MIKROTIK DI BIRO UMUM SEKRETARIAT DAERAH KALIMANTAN BARAT. *Journal of Electrical Engineering, Energy, and Information Technology (J3EIT)*, *9*(2). https://jurnal.untan.ac.id/index.php/j3eituntan/article/view/49092

Lase, F., & Halawa, N. (2022). Menjaga Dan Mendidik Anak Di Era Digital Terhadap Bahaya Pornografi. *Zadama: Jurnal Pengabdian Masyarakat*, *1*(1 SE-), Page 57-68. https://doi.org/10.56248/zadama.v1i1.21

Purwianti, L., Kesumahati, E., Wilyanto, A., Andelson, J., Jollin, Lien, T. P., Kevin, V. L., & Vanders, W. (2022). Penggunaan Internet Sehat Dan Aman Di Kalangan Pelajar. *National Conference for Community Service Project (NaCosPro)*, *4*(1), 276–283. https://doi.org/10.37253/NACOSPRO.V4I1.6955

Riyana Rahadjeng, I., & Ihsan Fajrin, A. (2021). Implementasi Manajemen Bandwidth Menggunakan Simple Queue Dan Filtering Content Pada Pusat Pelatihan Kerja Pengembangan Industri Jakarta Timur. *Jurnal Rekayasa Perangkat Lunak*, *2*(1). http://jurnal.bsi.ac.id/index.php/reputasi

Sari, M. W. (2024). *Dasar Jaringan Komputer*. UPY Press.

Sugandi, E. A., Juardi, D., & Ridha, A. A. (2023). IMPLEMENTASI METODE HIERARCHICAL TOKEN

BUCKET (HTB) DALAM MANAJEMEN BANDWITH JARINGAN INTERNET: *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*(4), 2749–2755. https://doi.org/10.36040/JATI.V7I4.7194

Sukaryati, L. N., Voutama, A., Karawang, U. S., & Ronggo, J. H. (2022). Penerapan Metode Simple Additive Weighting Pada Sistem Pendukung Keputusan Untuk Memilih Karyawan Terbaik. *Jurnal Ilmiah Matrik*, *24*(3), 260–267. https://doi.org/10.33557/JURNALMATRIK.V24I3.2029

Syafiq, A., Putra, A., & Asharudin, F. (2023). PENERAPAN MANAJEMEN BANDWIDTH DAN FILTERING WEBSITE MENGGUNAKAN LAYER 7 PADA MIKROTIK DI TAJIR.NET. *Jurnal Teknologi Informasi Dan Komputer*, *9*. https://doi.org/10.36002/jutik.v9i4.2530

Syarief, M., & Bardul, M. (2023). *View of IMPLEMENTASI SIMPLE QUEUE DAN FILTER WEBSITE UNTUK OPTIMASI MANAGEMENT BANDWIDTH PADA APARTEMEN MEDITERANIA*. https://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/view/6563/2703

Walidaini, B., Muhammad, A. M., Penulis, A., Bbppki, M., & Medan, K. (2018). PEMANFAATAN INTERNET UNTUK BELAJAR PADA MAHASISWA. *Jurnal Penulisan Bimbingan Dan Konseling*, *3*(1). https://jurnal.untirta.ac.id/index.php/JPBK/article/view/3200

Wuhi, A. U., Hariadi, F., & Uly, N. B. (2024). *View of Implementasi Web Filtering Firewall Untuk Mendukung Internet Sehat Di SMP Negeri 4 Mauliru*. Jurnal INOVATIF WIRA WACANA. https://ojs.unkriswina.ac.id/index.php/inovatif/article/view/801/496

Yunif Lukman Hakim, st, & HendroWijayanto, nd. (2024). Combination of Filtering and Switching Methods for Network Security from Pornographic Content. *International Journal of Computer and Information System (IJCIS)*, *5*(3), 132–191. https://ijcis.net/index.php/ijcis/article/view/173