



Simulasi Management Akses Pengguna Internet Sekolah Menggunakan Firewall Filter Rule dan Bandwidth Management Queue Tree

Alvin Bachtiar^{1*}, Agus Prihanto²

¹⁻²Teknik Informatika, Universitas Negeri Surabaya, Indonesia

alvinbachtiar.22024@mhs.unesa.ac.id¹, agusprihanto@unesa.ac.id²

*Penulis Korespondensi: alvinbachtiar.22024@mhs.unesa.ac.id

Abstract. The increasing integration of internet technology in educational institutions requires structured network governance to ensure that digital resources support academic activities effectively. Unrestricted access to online platforms often leads to non-academic usage such as online gaming and sosial media engagement during instructional hours, which may reduce learning concentration and degrade network performance. This research develops and evaluates a network access control simulation using a MikroTik RouterBoard RB951Ui-2HnD device. The system applies firewall filtering mechanisms, hotspot-based authentication, and bandwidth allocation strategies through Simple Queue configuration. Network segmentation is implemented to differentiate teacher and student access privileges. The study adopts a Research and Development (R&D) approach to design, configure, test, and evaluate the proposed system. Testing results indicate that the firewall configuration successfully restricts access to selected online games (Mobile Legends, Clash of Clans, Roblox) and sosial media platforms (YouTube, TikTok, Shopee, Instagram, Telegram). Furthermore, bandwidth management demonstrates effective traffic prioritization, ensuring more stable allocation for teacher accounts in accordance with configured maximum limits. The findings confirm that structured firewall and bandwidth policies can improve network discipline, enhance performance stability, and support a controlled digital learning environment in schools.

Keywords: Bandwith Management; Firewall; Hotspot; Mikrotik; School Network

Abstrak. Pemanfaatan internet di lingkungan pendidikan menuntut adanya pengelolaan jaringan yang terencana agar penggunaannya tetap selaras dengan tujuan pembelajaran. Akses yang tidak dibatasi berpotensi mendorong penggunaan non-akademik seperti permainan daring dan media sosial pada jam pelajaran, yang dapat menurunkan konsentrasi belajar serta memengaruhi kestabilan jaringan. Penelitian ini merancang dan menguji simulasi sistem pengendalian akses internet menggunakan perangkat MikroTik Routerboard RB951Ui-2HnD. Sistem dikonfigurasi melalui penerapan *firewall filtering*, *autentikasi hotspot*, serta pengaturan *bandwidth* menggunakan metode *Simple Queue*. Selain itu, dilakukan pemisahan hak akses antara guru dan siswa untuk menciptakan manajemen jaringan yang lebih terstruktur. Metode yang digunakan adalah *Research and Development (R&D)* dengan tahapan perancangan, implementasi, pengujian, dan evaluasi sistem. Hasil pengujian menunjukkan bahwa konfigurasi *firewall* mampu membatasi akses terhadap beberapa game daring dan platform media sosial tertentu. Manajemen *bandwidth* yang diterapkan juga berhasil memberikan prioritas akses yang lebih stabil bagi akun guru sesuai dengan parameter yang telah ditentukan. Dengan demikian, penerapan kebijakan *firewall* dan pengaturan *bandwidth* berbasis MikroTik terbukti mampu meningkatkan kontrol akses serta menjaga kestabilan jaringan di lingkungan sekolah.

Kata kunci: Firewall; Hotspot; Jaringan Sekolah; Manajemen Bandwith; MikroTik

1. LATAR BELAKANG

Transformasi digital dalam bidang pendidikan telah memperluas cara sekolah memanfaatkan teknologi sebagai sarana pembelajaran. Internet kini tidak hanya digunakan sebagai media komunikasi, tetapi juga sebagai sumber referensi akademik yang menyediakan artikel ilmiah, buku elektronik, video pembelajaran, hingga platform diskusi daring (Aidoo, 2024; Anwariyah et al., 2025). Keberadaan internet memungkinkan peserta didik dan pendidik memperoleh informasi secara cepat serta memperluas akses terhadap sumber belajar yang sebelumnya terbatas (Sasmita, 2020).

Meskipun demikian, pemanfaatan internet di sekolah tidak sepenuhnya memberikan dampak positif apabila tidak disertai pengelolaan yang memadai. Akses tanpa kontrol berpotensi mengarahkan siswa pada aktivitas non-akademik seperti permainan daring maupun penggunaan media sosial pada waktu pembelajaran berlangsung. Kondisi tersebut dapat mengurangi konsentrasi belajar sekaligus memengaruhi kualitas layanan jaringan karena penggunaan *bandwidth* yang tidak proporsional (Martin et al., 2025; Park et al., 2025; Robards, 2025; Lestari et al., 2024).

Beberapa penelitian menunjukkan bahwa penerapan kebijakan teknis melalui sistem keamanan jaringan dapat membantu membatasi akses terhadap konten yang tidak relevan dengan kegiatan belajar. Implementasi *firewall filtering* pada perangkat MikroTik terbukti mampu meningkatkan keamanan sekaligus mengendalikan penggunaan jaringan di lingkungan pendidikan (Aziz et al., 2024; Ma'mun & Muflih, 2025; Tamu et al., 2024). Selain itu, pengaturan manajemen *bandwidth* juga berperan penting dalam menjaga stabilitas koneksi serta mencegah terjadinya dominasi penggunaan oleh pengguna tertentu (Fauzan et al., 2025).

Sekolah sebagai institusi formal memiliki tanggung jawab untuk menciptakan lingkungan digital yang kondusif. Penggunaan MikroTik RouterOS memungkinkan administrator jaringan melakukan segmentasi akses berdasarkan peran pengguna, misalnya antara guru dan siswa. Strategi ini mendukung pengawasan penggunaan internet secara lebih terstruktur, termasuk melalui penerapan *firewall layer 7* untuk penyaringan konten dan *Quality of Service* (QoS) guna menjaga kualitas jaringan (Seyhan & Triloka, 2025; Fauzan et al., 2025; Rudiyanto & Asri, 2025).

Sekolah sebagai institusi formal memiliki tanggung jawab untuk menciptakan lingkungan digital yang kondusif. Penggunaan MikroTik RouterOS memungkinkan administrator jaringan melakukan segmentasi akses berdasarkan peran pengguna, misalnya antara guru dan siswa. Strategi ini mendukung pengawasan penggunaan internet secara lebih terstruktur, termasuk melalui penerapan *firewall layer 7* untuk penyaringan konten dan *Quality of Service* (QoS) guna menjaga kualitas jaringan (Seyhan & Triloka, 2025; Fauzan et al., 2025; Rudiyanto & Asri, 2025).

2. KAJIAN TEORITIS

Manajemen akses jaringan merupakan proses pengaturan lalu lintas data yang bertujuan untuk menjaga keamanan serta memastikan penggunaan sumber daya jaringan berlangsung secara efisien. Pengendalian ini dilakukan dengan menetapkan aturan tertentu pada perangkat jaringan agar hak akses pengguna dapat dibedakan sesuai kebutuhan. Melalui mekanisme

tersebut, penyalahgunaan jaringan dapat diminimalkan sekaligus meningkatkan kualitas layanan konektivitas (Hartono & Kholidah, 2024). Konsep ini juga selaras dengan penelitian yang dilakukan oleh Danang et al. (2025) yang menunjukkan bahwa pengelolaan akses jaringan yang tepat dapat mengurangi risiko penyalahgunaan dan mengoptimalkan penggunaan *bandwidth*.

MikroTik merupakan platform sistem operasi jaringan yang dirancang untuk menjalankan fungsi *routing* dan pengelolaan trafik secara terintegrasi. Awalnya dikembangkan sebagai perangkat lunak berbasis PC, MikroTik kemudian berkembang menjadi perangkat keras *routerboard* yang banyak digunakan dalam berbagai skala jaringan. Fitur yang tersedia mencakup *hotspot server*, *firewall*, manajemen *bandwidth*, serta konfigurasi *Quality of Service* (QoS), sehingga perangkat ini fleksibel dalam mendukung kebutuhan administrasi jaringan sekolah maupun institusi lainnya.

Dalam konteks pendidikan, pemanfaatan MikroTik tidak hanya berfungsi sebagai penghubung jaringan, tetapi juga sebagai alat pengendali akses internet yang memungkinkan penerapan kebijakan berbasis peran pengguna (Hartono & Kholidah, 2024; Rudiyanto & Asri, 2025).

Firewall merupakan sistem keamanan jaringan yang bertugas mengatur lalu lintas data masuk dan keluar berdasarkan seperangkat aturan yang telah ditentukan. Pada perangkat MikroTik, *firewall* dapat dikonfigurasi melalui fitur filter *rules*, *Network Address Translation* (NAT), serta *Layer 7 Protocol* yang memungkinkan analisis paket data hingga tingkat aplikasi (Putra et al., 2025).

Filtering konten dilakukan dengan cara membatasi akses terhadap situs atau layanan tertentu yang dianggap tidak relevan dengan tujuan pembelajaran. Penerapan *firewall* layer 7 memungkinkan identifikasi pola komunikasi aplikasi tertentu sehingga proses pemblokiran dapat dilakukan secara lebih spesifik dibandingkan metode berbasis alamat IP atau port saja (Madhloom et al., 2023). Dalam hal ini, konsep yang diusung oleh Danang & Mustofa (2026) tentang penggunaan teknik *real-time network traffic profiling* untuk memantau aktivitas jaringan dapat diterapkan untuk meningkatkan kontrol terhadap akses internet di sekolah. Teknologi seperti ini dapat mengidentifikasi pola komunikasi yang berisiko terhadap keamanan jaringan, seperti yang diungkapkan dalam penelitian mereka tentang *CLSTMNet Architecture* untuk mendeteksi dan mengurangi serangan DDoS yang juga berhubungan dengan pengelolaan akses jaringan.

Sejumlah penelitian menunjukkan bahwa implementasi *firewall* berbasis MikroTik efektif dalam meningkatkan keamanan jaringan sekaligus mengurangi akses terhadap konten yang tidak diinginkan di lingkungan sekolah (Aziz et al., 2024; Sianhar & Marhalim, 2025).

Pengelolaan *bandwidth* merupakan strategi untuk mendistribusikan kapasitas jaringan agar tidak terjadi ketimpangan penggunaan. Dengan menerapkan metode seperti *Simple Queue* atau *Queue Tree*, administrator dapat menentukan batas minimum (*Limit At*) dan batas maksimum (Max Limit) kecepatan akses bagi masing-masing kategori pengguna. Pendekatan ini memungkinkan prioritas tertentu diberikan kepada pengguna yang membutuhkan kestabilan akses lebih tinggi, seperti guru dalam proses pembelajaran daring (Fauzan et al., 2025; Rudiyanto & Asri, 2025).

Melalui kombinasi *firewall filtering* dan manajemen *bandwidth*, sistem jaringan sekolah dapat dikendalikan secara lebih efektif sehingga tercipta lingkungan digital yang aman, stabil, dan mendukung kegiatan akademik. Seperti yang disarankan oleh Danang et al. (2024), dengan memanfaatkan teknologi berbasis IoT, pengelolaan jaringan dapat dilakukan dengan lebih efisien, bahkan memungkinkan pemantauan kualitas dan stabilitas jaringan secara *real-time* untuk mendukung kegiatan akademik yang lebih baik.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan *Research and Development* (R&D) karena berorientasi pada perancangan, pengembangan, serta pengujian suatu sistem manajemen akses jaringan berbasis MikroTik. Metode ini dipilih karena penelitian tidak hanya bertujuan menganalisis permasalahan, tetapi juga menghasilkan produk berupa konfigurasi sistem yang dapat diterapkan secara langsung di lingkungan sekolah. Dalam konteks ini, produk yang dikembangkan berupa sistem pengendalian akses internet melalui penerapan *firewall filtering* dan manajemen *bandwidth* yang dirancang untuk membedakan hak akses antara guru dan siswa.

Proses penelitian diawali dengan analisis kebutuhan jaringan di lingkungan sekolah untuk mengidentifikasi permasalahan yang berkaitan dengan penggunaan internet, seperti akses terhadap aplikasi non-akademik dan ketidakseimbangan distribusi *bandwidth*. Hasil analisis tersebut menjadi dasar dalam menyusun rancangan sistem yang meliputi perencanaan topologi jaringan, segmentasi pengguna, serta penyusunan aturan *firewall* dan parameter manajemen *bandwidth*. Perangkat yang digunakan dalam penelitian ini adalah MikroTik *Routerboard* RB951Ui-2HnD yang dikonfigurasi melalui aplikasi Winbox untuk mengatur alamat IP, DHCP Server, serta rule *firewall* filter sesuai kebutuhan sistem.

Setelah tahap perancangan selesai, dilakukan implementasi konfigurasi secara bertahap agar sistem dapat beroperasi sesuai dengan desain yang telah disusun. Konfigurasi meliputi pembuatan aturan pemblokiran aplikasi tertentu melalui *firewall filter rules* serta penerapan manajemen *bandwidth* menggunakan metode *Simple Queue* dengan pengaturan nilai Limit At dan Max Limit. Selanjutnya, dilakukan pengujian sistem dengan membandingkan kondisi jaringan sebelum dan sesudah implementasi. Pengujian dilakukan melalui uji akses terhadap aplikasi yang ditargetkan untuk dibatasi serta pengukuran kecepatan *upload* dan *download* untuk melihat efektivitas pengaturan *bandwidth*.

Hasil pengujian kemudian dianalisis untuk menilai keberhasilan sistem dalam mengontrol akses internet dan menjaga kestabilan jaringan. Apabila ditemukan ketidaksesuaian antara hasil implementasi dan tujuan penelitian, dilakukan penyesuaian konfigurasi hingga diperoleh sistem yang optimal. Dengan tahapan tersebut, metode *Research and Development* memungkinkan penelitian ini menghasilkan solusi teknis yang aplikatif dan relevan dengan kebutuhan pengelolaan jaringan di lingkungan sekolah.

4. HASIL DAN PEMBAHASAN

Hasil

Implementasi adalah tahap di mana perangkat keras dan perangkat lunak yang telah dirancang sebelumnya dapat terkonfigurasi agar dapat beroperasi sesuai dengan tujuan yang telah dirancang sebelumnya, Proses ini melibatkan pengaturan perangkat keras seperti menghubungkan Mikrotik *Router ISP*, *access point* dan *switch* menggunakan kabel *ethernet* kemudian dilanjutkan dengan mengonfigurasi *firewall*. Setelah implementasi selesai langkah terakhir adalah pengujian *packet filtering* dengan cara membuka aplikasi yang akan diblokir

a. Instalasi Winbox

Aplikasi winbox bersifat gratis dan dapat diunduh melalui situs resmi mikrotik <https://mikrotik.com/download>. Untuk melakukan konfigurasi mikrotik dengan menggunakan aplikasi winbox yang sudah selesai di unduh kemudian pada tab bagian bawah pilih neighbors, pilih mac address setelah itu klik tombol *connect* pada bagian tab atas. Secara *default* autentikasi pada mikrotik cukup ketikkan admin dan *password* dikosongkan saja

b. Konfigurasi IP Address

Tahap ini merupakan suatu langkah untuk menentukan pengalamatan *IP address* pada *interface* yang akan di gunakan, Perangkat Mikrotik *Routerboard RB951Ui-2HnD* memiliki 5 port *ethernet*

c. Konfigurasi DHCP Server

Setelah melakukan pengalamatan *IP address* pada *interface* perangkat Mikrotik, langkah selanjutnya adalah melakukan konfigurasi *dhcp server*. DHCP (*Dyanamic Host Configuration Protocol*) server merupakan sebuah instrumen komputer mampu mendistribusikan Alamat *IP address server* ke seluruh perangkat *client (dhcp client)* yang terhubung pada sebuah jaringan.

Pembahasan

Pada tahap akhir setelah implementasi sistem adalah pengujian sistem. Tahap ini sangat penting untuk mengetahui kinerja implementasi pemblokiran aplikasi menggunakan *firewall filter rules* sebelum maupun sesudah. Tahap pengujian ini dilakukan dengan cara membuka aplikasi sebelum terkonfigurasi *firewall* dan sesudah dengan sistem *firewall*

a. Sebelum Implementasi

Tahap awal sebelum melakukan implementasi pemblokiran aplikasi adalah mencoba mengakses semua aplikasi yang akan dibuka dan mencari sumber port dari aplikasi tersebut, Berikut merupakan hasil dari uji coba akses aplikasi.

Tabel 1. Hasil Sebelum Implementasi *Firewall* Filter

NO	Kategori	Aplikasi	Dapat Diakses	Terblokir
1	Game Online	Mobile Legends: Bang Bang	√	
2	Game Online	Clash Of Clans	√	
3	Game Online	Roblox	√	
4	Sosial Media	TikTok	√	
5	Sosial Media	Shopee	√	
6	Sosial Media	Youtube	√	
7	Sosial Media	Instagram	√	
8	Sosial Media	Telegram	√	

b. Setelah Implementasi

Setelah melakukan konfigurasi *firewall filter rules*, Langkah selanjutnya adalah melakukan pengujian pemblokiran aplikasi untuk menentukan keberhasilan dari *packet filtering* yang telah di konfigurasi pengujian ini hasil dari pengujian

Tabel 2. Hasil Sesudah Implementasi *Firewall* Filter

NO	Kategori	Aplikasi	Dapat Diakses	Terblokir
1	Game Online	Mobile Legends: Bang Bang		√
2	Game Online	Clash Of Clans		√
3	Game Online	Roblox		√
4	Sosial Media	TikTok		√
5	Sosial Media	Shopee		√
6	Sosial Media	Youtube		√
7	Sosial Media	Instagram		√
8	Sosial Media	Telegram		√

Konfigurasi *firewall filter rules* digunakan untuk menentukan suatu paket data dapat masuk atau tidak ke dalam sistem *router* MikroTik, paket data yang akan ditangani fitur filter ini adalah paket data yang ditunjukkan pada salah satu *interface router*, Fitur di dalam *filter rules* ini memiliki 3 buah *Chain* yaitu

a. *Forward*

Forward digunakan untuk memproses trafik paket data yang hanya melewati *router*

b. *Input*

Input digunakan untuk memproses trafik paket data yang masuk ke dalam *router* melalui *interface* yang ada di *router*. Apabila bertentangan dengan aturan atau *rule chain Input*, paket tidak dapat melewati *router*

c. *Output*

Output digunakan untuk memproses trafik paket data yang keluar dari *router* dan meninggalkan melalui salah satu *interface* atau merupakan kebalikan dari *chain Input*

Adapun cara untuk mengonfigurasi terdapat menu IP > *firewall* > pilih tab *Filter Rules* > klik tanda (+) kemudian konfigurasi sesuai dengan tabel di bawah ini

Tabel 3. Konfigurasi *Firewall* Filter

NO	Aplikasi	Port TCP	Port UDP
1	Mobile Legend	5000-5221,5224-5227,5229-5241,5243-5287,5289-5352,5354-5509,5517-5520-5529-5551-5569-5601-5700-9000-9010 9443,10003,30000-30900	2702,3702,4001-4009,5000-5221,5224-5241,5243-5287, 5289-5352, 5354-5509
2	Clash Of Clans	9330-9340	9330-9340
3	Roblox	49152-65535	49152-65535
4	TikTok	Untuk sosial melakukan pemblokiran melalui konten di <i>filter rule</i> dengan cara memblokir <i>address</i> : Tiktok.com	Untuk sosial media melakukan pemblokiran melalui konten di <i>filter rule</i> dengan cara memblokir <i>address</i> : Tiktok.com
5	Shopee	Untuk sosial media melakukan pemblokiran melalui konten di <i>filter rule</i> dengan cara memblokir <i>address</i> : Shopee	Untuk sosial media melakukan pemblokiran melalui konten di <i>filter rule</i> dengan cara memblokir <i>address</i> : Shopee
6	Youtube	Untuk sosial media melakukan pemblokiran melalui konten di <i>filter rule</i> dengan cara memblokir <i>address</i> : Youtube	Untuk sosial media melakukan pemblokiran melalui konten di <i>filter rule</i> dengan cara memblokir <i>address</i> : Youtube
7	Instagram	Untuk sosial media melakukan pemblokiran melalui konten di <i>filter rule</i> dengan cara memblokir <i>address</i> : Instagram	Untuk sosial media melakukan pemblokiran melalui konten di <i>filter rule</i> dengan cara memblokir <i>address</i> : Instagram

- 8 Telegram Untuk sosial media melakukan pemblokiran melalui konten di *filter rule* dengan cara memblokir *address*: Telegram
- Untuk sosial media melakukan pemblokiran melalui konten di *filter rule* dengan cara memblokir *address*: Telegram

Setelah *user* berhasil *login hotspot*, sistem secara otomatis menerapkan manajemen *bandwidth* menggunakan *Simple Queue*. Dari hasil pengujian di menu *queue list*, terlihat bahwa trafik Siswa *upload* dan *download* dibatasi sesuai konfigurasi sehingga tidak ada pengguna yang mendominasi *bandwidth*

Name	Parent	Packet...	Limit At (bi...	Max Limit (...Avg Ra...	Queued Bytes	Bytes	Packets
Bandwidth Guru	global	Downlo...	5M	10M	0 bps	0 B	0 B
Bandwidth Siswa	global	Downlo...	3M	6M	0 bps	0 B	0 B
Bandwidth Guru	global	Uploa...	5M	10M	0 bps	0 B	0 B
Bandwidth Siswa	global	Uploa...	3M	6M	0 bps	0 B	0 B

Gambar 1. Pembatasan Limit *Queue Tree*

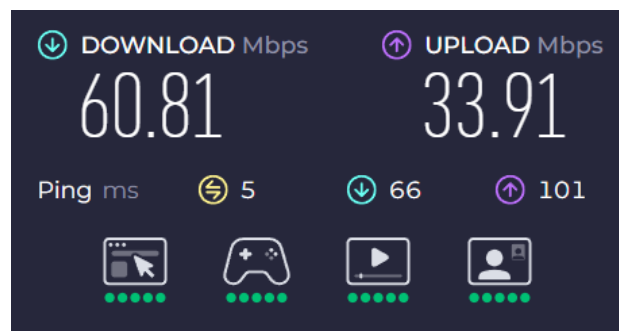
Pengujian *firewall* dilakukan dengan memisahkan trafik *upload* dan *download* menggunakan *rule Forward*. Hasilnya terlihat pada nilai bytes dan packets yang bertambah menandakan bahwa *firewall* aktif dan mampu mengontrol lalu lintas data sesuai kebijakan jaringan

#	Action / Chain	Src. Address	Proto...	In. Interf...	Out. Inte...	Bytes	Packets	Dst. Address
0	Download Guru					28.0 MiB	33 827	192.168.1.0/...
1	Upload Guru	192.168.1.0/...				24.1 MiB	32 340	
2	Download Siswa					0 B	0	192.168.2.0/...
3	Upload Siswa	192.168.2.0/...				0 B	0	

Gambar 2. *Firewall Mangle* Mengontrol Sesuai Kebijakan Jaringan

a. Sebelum Implementasi

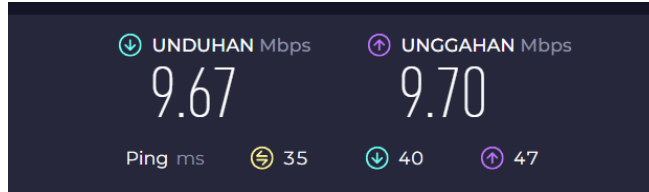
Ketika di nonaktifkan atau *disabled* kita akan uji *download* dan *uploadnya* di *speed test* apakah tetap berjalan sesuai pembatasan akses *scenario* pengujian



Gambar 3. Hasil *Download* dan *Upload* sebelum Implementasi

b. Sebelum Implementasi

Hasil pengujian menunjukkan bahwa sistem *hotspot* Mikrotik yang dirancang mampu mengontrol akses *bandwidth*, dan keamanan jaringan secara efektif. Di buktikan dengan hasil *speed test* yang stabil dan konsisten pada beberapa kali pengujian



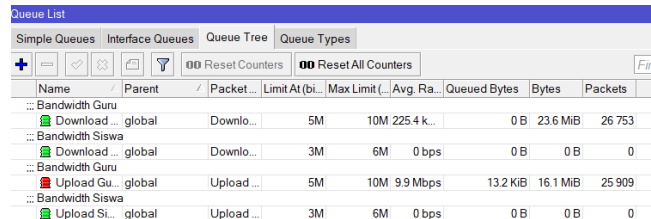
Gambar 4. Hasil *Download* dan *Upload* setelah implementasi

Menunjukkan konfigurasi *Queue Tree* yang diterapkan pada Mikrotik. Pembagian *bandwidth* dilakukan melalui *parent queue* dengan pengaturan *Limit At* dan *Max Limit* yang berbeda untuk setiap jenis pengguna Guru diberikan prioritas *bandwidth* lebih tinggi dibandingkan siswa untuk menjamin kestabilan akses jaringan

Tabel 4. Pembagian *Bandwidth*

Pengguna	Jenis Trafik	Parent Queue	LimitAt (Mbps)	MaxLimit (Mbps)
Guru	Download	_global	5	10
Siswa	Download	_global	3	6
Guru	Upload	_global	5	10
Siswa	Upload	_global	3	6

Hasil pengujian membuktikan bahwa konfigurasi berhasil diterapkan ditandai dengan *bandwidth* guru yang lebih stabil dan sesuai dengan nilai *Max limit* yang telah ditentukan



Gambar 5. Hasil *Download* dan *Upload Queue Tree*

5. KESIMPULAN DAN SARAN

Berdasarkan hasil implementasi *management* akses internet simulasi di sekolah maka dapat disimpulkan bahwa sistem ini dapat melakukan pemblokiran game online yaitu Mobile Legends Bang Bang, Clash of Clans, Roblox. Tidak hanya game online, adapun sosial media yaitu Youtube, Tiktok, Shopee, Telegram. Implementasi Mikrotik RB951Ui-2HnD sebagai manajemen jaringan sekolah berhasil menciptakan sistem jaringan yang terstruktur melalui pemisahan jaringan guru dan siswa. Pemisahan ini mendukung pengelolaan akses internet yang lebih terkontrol sesuai peran pengguna

Berdasarkan kesimpulan yang telah diperoleh, maka saran yang dapat diberikan adalah dengan adanya pembatasan penggunaan game online dan sosial media dengan *firewall filter rules* sebagaimana telah dilakukan, di harapkan dapat digunakan secara berkelanjutan mengingat pembatasan akses pada jaringan WI-FI sangatlah penting untuk dilakukan agar dapat mengontrol penggunaan internet para siswa. Terkait pemisahan jaringan Guru dan Siswa sekolah disarankan untuk menerapkan pemisahan jaringan guru dan siswa secara nyata dengan memanfaatkan *VLAN* atau *Virtual Access Point (VAP)*, agar keamanan jaringan dan pengelolaan akses dapat lebih optimal sebagaimana hasil yang diperoleh pada penelitian ini

DAFTAR REFERENSI

- Aidoo, B., & Chebure, A. (2024). Integrating ICT to adopt online learning in teacher education in Ghana. *Education Sciences*. <https://doi.org/10.3390/educsci14121313>
- Anwariyah, L., & Yasin, N. A. (2025). Transformasi pembelajaran di era digital: Pemanfaatan internet sebagai sumber belajar yang inovatif. *Jurnal Kajian Dan Inovasi Ilmu (JKII)*, 1(1). <https://doi.org/10.64123/jkii.v1.i1.4>
- Danang, D., & Mustofa, Z. (2026). CLSTMNet architecture: A CNN–LSTM-based hybrid deep learning model for DDoS attack detection and mitigation in network security. *Journal of Artificial Intelligence and Technology*. <https://doi.org/10.37965/jait.2025.0887>
- Danang, D., Santoso, A. B., & Dewi, M. U. (2025). CICA framework: Harnessing CSR, AI, and blockchain for sustainable digital culture. *International Journal of Advanced Computer Science & Applications*, 16(11). <https://doi.org/10.14569/IJACSA.2025.0161135>
- Danang, D., Setiawan, N. D., & Siswanto, E. (2024). Pemanfaatan teknologi internet of things untuk monitoring kualitas air sungai di wilayah perkotaan. *Journal of New Trends in Sciences*, 2(1), 23–34. <https://doi.org/10.59031/jnts.v2i1.784>
- Hartono, R., & Kholidah, M. N. (2024). Sistem user management menggunakan Mikrotik RouterOS untuk mengontrol akses internet siswa pada SMK Miftakhul Huda Way Areng berbagai sektor, termasuk pendidikan. *Jurnal Ilmiah Informasi*.
- Lestari, Y. E., Pudir, Y. A., & Wibowo, V. M. (2024). The impact of digital learning policies on educational equity in rural Indonesian schools. 2.
- Madhloom, J. K., Noori, Z. H., Ebis, S. K., Hassen, O. A., & Darwish, S. M. (2023). An information security engineering framework for modeling packet filtering firewall using neutrosophic Petri nets. *Computers*, 12. <https://doi.org/10.3390/computers12100202>
- Martin, F., Long, S., Haywood, K., Xie, K., & Martin, F. (2025). Digital distractions in education: A systematic review of research on causes, consequences, and prevention strategies. *Educational Technology Research and Development*, 73(6), 3423–3451. <https://doi.org/10.1007/s11423-025-10550-6>

- Ma'mun, A. S., & Muflih, G. Z. (2025). Implementasi web filtering firewall untuk keamanan pada jaringan internet di Pondok Pesantren Al Hidayah Kebumen. *SKANIKA*, 8, 46–59. <https://doi.org/10.36080/skanika.v8i1.3298>
- Park, J., Paxtle-Granjeno, J., Wook, M., Shin, M., & Wilson, E. (2025). Preventing digital distraction in secondary classrooms: A quasi-experimental study. *Computers & Education*, 227(August 2024), 105223. <https://doi.org/10.1016/j.compedu.2024.105223>
- Prasetyo, F., Putra, E., Arissandi, D. E., Rofiqi, A., & Hidayat, M. F. (2025). Pemanfaatan Mikrotik dalam manajemen bandwidth pada jaringan sekolah. *Jurnal Informatika*
- Prasetyo, F., Putra, E., Dafid, M., & Syafi, I. (2025). Firewall implementation as a computer network security strategy for data protection. *Brilliance: Research of Artificial Intelligence*, 5(1), 291–297. <https://doi.org/10.47709/brilliance.v5i1.6162>
- Robards, B., Goring, J., Hendry, N. A., Robards, B., & Goring, J. (2025). Guiding young people's social media use in school policies: Opportunities, risks, moral panics, and imagined futures. *Journal of Youth Studies*, 6261, 1–17. <https://doi.org/10.1080/13676261.2025.2468477>
- Roberts, J., Umbu, T., Alfa, P., Leo, R., Marten, L., Ratu, D., Informatika, T., Kristen, U., Wacana, W., Jl, A., No, R. S., & Waingapu, K. K. (2024). Implementasi manajemen bandwidth dan filtering firewall. *Jurnal Mahasiswa Teknik Informatika*, 8(3), 4247–4255. <https://doi.org/10.36040/jati.v8i3.9885>
- Rudiyanto, R., Asri, S. D., Studi, P., Informatika, T., & Dian, U. (2025). Optimasi bandwidth jaringan Wi-Fi sekolah berbasis Mikrotik menggunakan Queue Tree dan QoS. *Journal of Computer Science and Informatics Engineering*, 04(4), 334–344. <https://doi.org/10.55537/cosie.v4i4.1284>
- Sasmita, R. S. (2020). Research & learning in primary education: Pemanfaatan internet sebagai sumber belajar. *Jurnal Ilmu Pendidikan*, 2. <https://doi.org/10.31004/jpdk.v1i2.603>
- Triloka, J. (2025). Implementation of Mikrotik firewall and QoS for secure and efficient internet networking. *J. teknol. inf. pendidik.*, 18(2), 1097–1109. <https://doi.org/10.24036/jtip.v18i2.1056>