JUNIF: Jurnal Nasional Informatika

p-ISSN: 2774-3497
e-ISSN: 2774-3500

Vol. 7 No. 2, 30 Oktober 2026, pp. 78-90

IMPLEMENTASI FIREWALL MIKROTIK MENGGUNAKAN LAYER 7 PROTOCOL DALAM UPAYA PENINGKATAN KEAMANAN JARINGAN PADA MADRASAH IBTIDAIYAH FATAHILLAH

PENULIS [1)]**Deva Muhammad Insanu Afif,** [2)]**Astried Silvanie**

ABSTRAK

Di era digital ini, keamanan jaringan sangat penting dan menjadi prioritas utama, terutama pada lingkungan sekolah yang menggunakan internet untuk mendukung aktivitas pembelajaran. Penelitian ini dilakukan di Madrasah Ibtida'iyah Fatahillah dengan maksud meningkatkan keamanan jaringan menggunakan firewall Mikrotik RouterBoard RB941-2nD. Penelitian dilakukan dengan deskriptif kualitatif; peneliti bermodalkan observasi, wawancara, dan dokumentasi serta disertai uji coba sederhana sebelum dan sesudah konfigurasi. Penggunaan aplikasi Winbox pada sempurnanya adalah sebagai media konfigurasi Mikrotik. Kelengkapan fitur serta kemudahan fitur yang ditawarkannya telah menunjang keperluan dan kebutuhan para penggunanya. Firewall dapat diisi rules seperti Layer 7 Protocol yang dipakai untuk memblokir situs yang tidak sesuai kegiatan pembelajaran, seperti akses media sosial dan situs hiburan. Hasil penelitian bahwa penggunaan firewall berhasil membatasi akses situs tertentu dan membuat penggunaan internet lebih aman serta terarah. Ada beberapa kendala yang dijumpai, seperti konfigurasi yang relatif rumit dan adanya tambahan beban pada perangkat atau sempitnya bandwidth. Secara keseluruhan, penerapan Mikrotik Firewall dengan tipe Layer 7 Protocol terbukti efektif membantu sekolah menjaga keamanan jaringan.

Kata Kunci *Keamanan Jaringan; Firewall; Mikrotik RB941-2^{nD}; Winbox; Layer 7 Protocol; Madrasah Ibtidaiyah;*

AFILIASI

Prodi, Fakultas [1,2)] Program Studi Teknik Informatika, Fakultas Ilmu Komputer.
Nama Institusi [1,2)] Institut Bisnis dan Informatika Kosgoro 1957.
Alamat Institusi [1,2)] Jl. Moh Kahfi II, Srengseng Sawah, Jagakarsa, Jakarta Selatan, DKI Jakarta.

KORESPONDENSI

Penulis Deva Muhammad Insanu Afif
Email deva.smartfren2016@gmail.com

LICENSE

This work is licensed under a Creative Commons Attribution 4.0 International License.

DOI : https://doi.org/10.55122/junif.v7i2.2432

I. PENDAHULUAN

Internet telah menjadi bagian integral dalam aktivitas pembelajaran di sekolah. Jika dahulu sumber utama pembelajaran terbatas pada buku dan papan tulis, kini hampir seluruh proses pendidikan dapat dibantu oleh jaringan internet. Guru dapat menyiapkan materi yang lebih lengkap, siswa dan mahasiswa lebih mudah mencari referensi tambahan, serta pengumpulan tugas dapat dilakukan tanpa pertemuan tatap muka. Meskipun menyediakan berbagai kemudahan, pemanfaatan internet di lingkungan sekolah juga menimbulkan permasalahan baru. Di Madrasah Ibtidaiyah Fatahillah, misalnya, terdapat kecenderungan sebagian siswa menggunakan akses internet untuk aktivitas yang tidak berkaitan dengan pembelajaran, seperti membuka media sosial, menonton konten yang tidak pantas, atau bermain game online. Perilaku tersebut tidak hanya mengurangi fokus belajar tetapi juga membebani kapasitas jaringan sehingga menyebabkan koneksi menjadi lambat. Kondisi ini menunjukkan bahwa penyediaan akses internet saja tidak menjamin pemanfaatan yang tepat; diperlukan mekanisme pengendalian agar penggunaan internet lebih terarah dan aman.

Salah satu solusi pengendalian akses yang dapat diterapkan adalah pemasangan firewall. Secara konseptual, firewall berfungsi sebagai penjaga gerbang jaringan yang dapat menentukan lalu lintas mana yang diizinkan atau diblokir. Pada konteks sekolah, firewall dapat memfilter paket data masuk dan keluar sehingga akses internet lebih sesuai dengan kebutuhan pembelajaran. Perangkat populer yang sering digunakan untuk tujuan ini adalah Mikrotik, karena menawarkan fitur lengkap, biaya relatif terjangkau, serta konfigurasi yang fleksibel. Dalam Mikrotik terdapat fitur Layer 7 Protocol yang memungkinkan pengenalan pola payload aplikasi (application layer) sehingga dapat membedakan jenis aktivitas internet berdasarkan pola data, bukan hanya sekadar alamat IP atau domain. Dengan memanfaatkan Layer 7 Protocol, administrator jaringan sekolah dapat memblokir kategori situs hiburan atau media sosial sekaligus tetap mengizinkan akses ke situs pendidikan. Pendekatan ini diharapkan meningkatkan keamanan, kestabilan, dan efektivitas pemanfaatan internet untuk proses belajar-mengajar.

Firewall merupakan komponen penting dalam sistem keamanan jaringan yang berfungsi sebagai pelindung utama dari akses tidak sah. Melalui mekanisme penyaringan paket data, firewall memastikan hanya lalu lintas yang sesuai kebijakan yang dapat melewati jaringan. Dengan menggunakan IPTables, administrator dapat membuat aturan pemblokiran atau pengizinkan akses sesuai kebutuhan, sehingga ancaman dari luar seperti malware dan intrusi dapat diminimalkan[1]. Penerapan firewall dengan pfSense juga banyak dilakukan di berbagai institusi karena memiliki konfigurasi yang fleksibel dan tampilan antarmuka yang ramah pengguna. Sistem ini membantu administrator dalam melakukan pemantauan aktivitas jaringan secara real-time, serta memberikan perlindungan berlapis terhadap serangan siber. Dengan pengaturan yang baik, kinerja jaringan menjadi lebih stabil dan aman untuk mendukung kegiatan operasional[2]. Firewall Mikrotik juga banyak digunakan pada jaringan komunitas maupun sekolah, karena memiliki fitur lengkap untuk pembatasan akses dan pengaturan bandwidth. Melalui konfigurasi filtering dan NAT, administrator dapat mengatur prioritas akses pengguna, memblokir situs berbahaya, serta menjaga kestabilan koneksi. Hal ini membuktikan bahwa firewall menjadi salah satu kunci utama dalam menjaga keamanan jaringan modern[3].

Layer 7 Protocol bekerja pada lapisan aplikasi dari model OSI dan memiliki kemampuan untuk mengenali pola data berdasarkan isi konten. Teknologi ini membuat firewall lebih cerdas dalam melakukan analisis lalu lintas, sehingga mampu memblokir situs atau aplikasi tertentu tanpa perlu bergantung pada alamat IP atau port. Dengan kemampuan ini, administrator dapat mengelola jaringan lebih efektif dan menyesuaikan kebijakan sesuai kebutuhan pengguna[4]. Implementasi Layer 7 Protocol pada perangkat Mikrotik juga banyak diterapkan di sektor pendidikan maupun kantor. Dengan kombinasi metode RAW dan firewall rule, sistem dapat mendeteksi pola akses ke situs hiburan atau media sosial yang tidak diperlukan. Hal ini membantu menjaga efisiensi bandwidth serta meningkatkan keamanan jaringan secara menyeluruh. Selain itu, metode ini mudah diterapkan tanpa memerlukan perangkat tambahan[5]. Penggunaan Layer 7 Protocol bersama sistem

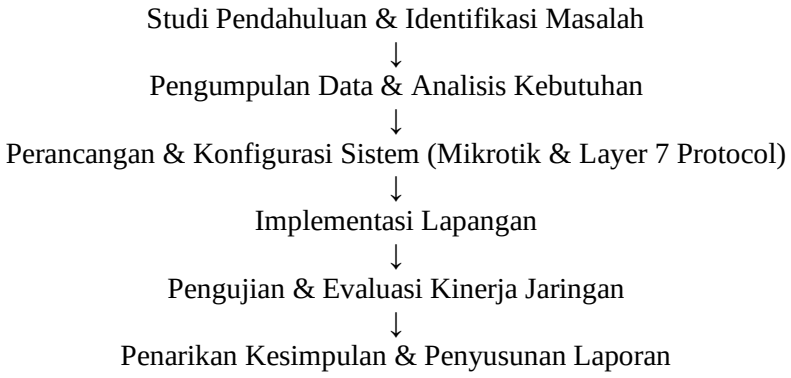
proxy juga dapat memperkuat keamanan jaringan. Kombinasi ini memungkinkan deteksi pola data berbahaya seperti aktivitas malware atau konten berisiko, sehingga administrator dapat melakukan tindakan pencegahan lebih awal. Pendekatan tersebut terbukti meningkatkan stabilitas dan efisiensi jaringan, terutama di lingkungan dengan banyak pengguna aktif seperti sekolah atau kampus[6].

Keamanan jaringan di lingkungan pendidikan merupakan aspek vital dalam mendukung kegiatan pembelajaran berbasis digital. Sekolah atau kampus perlu memastikan setiap pengguna jaringan memiliki batasan akses yang jelas agar tidak terjadi penyalahgunaan. Dengan menerapkan sistem firewall berbasis Mikrotik, administrator dapat mengatur kebijakan akses, menjaga kestabilan bandwidth, dan meminimalkan risiko serangan dari luar jaringan[7]. Penerapan firewall adaptif juga terbukti efektif dalam membatasi akses ke situs yang tidak relevan. Melalui metode DNS filtering dan kontrol konten, sekolah dapat mengelola jaringan yang ramah pembelajaran. Sistem ini tidak hanya berfungsi sebagai alat teknis pengamanan, tetapi juga sebagai media edukasi bagi siswa agar menggunakan internet dengan bijak dan produktif[8]. Keamanan jaringan yang baik juga dapat meningkatkan kualitas pembelajaran di laboratorium komputer. Dengan pemantauan lalu lintas secara rutin dan pembatasan terhadap aktivitas mencurigakan, administrator dapat memastikan setiap perangkat bekerja optimal. Implementasi firewall membantu menjaga konektivitas tetap stabil, bebas gangguan, dan aman dari potensi serangan eksternal[9].

Berdasarkan uraian tersebut, penelitian ini bertujuan menerapkan firewall Mikrotik menggunakan metode Layer 7 Protocol di Madrasah Ibtidaiyah Fatahillah. Tujuan khusus penelitian adalah mengukur efektivitas metode ini dalam membatasi akses ke situs yang tidak mendukung kegiatan pembelajaran serta menilai pengaruhnya terhadap keamanan dan kenyamanan jaringan. Hasil penelitian diharapkan menjadi referensi bagi institusi pendidikan lain yang ingin mengelola akses internet secara lebih bijaksana dan efisien.

II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif yang bertujuan untuk menggambarkan dan menganalisis penerapan firewall Mikrotik menggunakan *Layer 7 Protocol* dalam upaya peningkatan keamanan serta efisiensi jaringan di Madrasah Ibtidaiyah Fatahillah. Secara rinci, tahapan-tahapan yang ditempuh dalam pelaksanaan penelitian ini digambarkan melalui alur berikut:



Gambar 1. Diagram Alur

2.1 Studi Pendahuluan dan Identifikasi Masalah

Tahap awal dilakukan untuk mengenali kondisi eksisting jaringan di Madrasah Ibtidaiyah Fatahillah. Pada tahap ini, diidentifikasi adanya permasalahan terkait penggunaan internet oleh siswa yang kerap digunakan untuk mengakses situs non-edukasi (seperti media sosial dan hiburan), yang berimbas pada ketidakstabilan bandwidth dan penurunan fokus pembelajaran.

2.2 Pengumpulan Data

Metode pengumpulan data dilakukan melalui tiga pendekatan utama:

- Observasi Lapangan: Mengamati langsung pola penggunaan internet, kondisi perangkat keras jaringan, serta kendala teknis sebelum sistem keamanan diterapkan.
- Wawancara: Melakukan tanya jawab dengan guru dan staf IT sekolah guna mengetahui kebutuhan spesifik kebijakan akses internet di lingkungan sekolah.
- Studi Dokumentasi: Menelaah topologi jaringan yang ada, spesifikasi perangkat router, serta dokumen pendukung terkait kebijakan pemanfaatan internet madrasah.

2.3 Perancangan dan Konfigurasi Sistem

Tahap perancangan sistem meliputi penyiapan perangkat keras utama yaitu Mikrotik RouterBoard RB941-2nD. Konfigurasi dilakukan menggunakan aplikasi Winbox dengan tahapan sistematis:

- Pengaturan alamat IP dasar (DHCP Server dan Gateway).
- Pembuatan pola pencocokan (regular expression) pada menu Layer 7 Protocols untuk mengenali trafik situs hiburan atau media sosial.
- Penerapan aturan penyaringan (Filter Rules) dengan chain forward dan aksi pemblokiran (drop) agar situs non-pembelajaran tidak dapat diakses.

2.4 Implementasi Lapangan

Konfigurasi yang telah diuji secara terbatas kemudian diterapkan secara menyeluruh pada jaringan sekolah yang mencakup laboratorium komputer, ruang guru, ruang kepala sekolah, serta area Wi-Fi umum. Pada tahap ini, seluruh trafik data dari berbagai ruangan dikendalikan secara terpusat melalui perangkat Mikrotik.

2.5 Pengujian dan Evaluasi

Evaluasi dilakukan selama periode waktu tertentu untuk mengukur efektivitas sistem yang telah dibangun. Pengujian menitikberatkan pada:

- Stabilitas koneksi internet di lingkungan sekolah.
- Keberhasilan pemblokiran situs non-edukatif menggunakan fitur Layer 7 Protocol.
- Efisiensi penggunaan bandwidth menggunakan alat pemantau lalu lintas jaringan seperti fitur Torch, Traffic Monitor, dan Log Activity pada Winbox.

2.6 Penarikan Kesimpulan

Tahap akhir dari metodologi ini adalah menganalisis hasil perbandingan kondisi jaringan sebelum dan sesudah penerapan firewall, untuk kemudian ditarik simpulan apakah implementasi ini berhasil menjawab tujuan penelitian dalam meningkatkan keamanan dan efisiensi jaringan madrasah.

.

III. HASIL DAN PEMBAHASAN

3.1 Penerapan Mikrotik Routerboard RB942-2nD

Penerapan sistem firewall di Madrasah Ibtidaiyah Fatahillah dilakukan dengan menggunakan perangkat Mikrotik RouterBoard RB941-2nD. Perangkat ini dipasang sebagai pusat pengendali koneksi antara modem penyedia internet dengan jaringan lokal sekolah yang mencakup ruang guru, laboratorium komputer, dan beberapa ruang kelas. Sebelum Mikrotik digunakan, jaringan sekolah masih menggunakan router bawaan dari penyedia layanan internet tanpa sistem pengaturan lalu lintas. Akibatnya, koneksi internet sering tidak stabil dan sulit dipantau oleh pihak sekolah.

Proses pemasangan dilakukan di ruang server kecil yang menjadi titik utama distribusi jaringan. Mikrotik dihubungkan langsung ke modem utama, kemudian dari perangkat tersebut koneksi diteruskan ke switch yang menyalurkan akses ke seluruh ruangan. Jalur kabel disusun ulang agar lebih teratur dan mudah dalam proses pemeliharaan. Pada tahap ini, fokus utama adalah memastikan seluruh perangkat di lingkungan sekolah dapat terhubung ke jaringan melalui Mikrotik dengan koneksi yang stabil dan terpusat.



Gambar 2. Mikrotik RouterBoard RB941-2nD

Perangkat ini dipilih karena memiliki ukuran kecil, konfigurasi yang mudah dilakukan, dan sudah mendukung fitur firewall bawaan. Mikrotik RouterBoard RB941-2nD cocok digunakan di lingkungan sekolah yang memiliki jumlah pengguna tidak terlalu banyak namun membutuhkan kontrol jaringan yang terpusat. Selain itu, sistem operasinya, RouterOS, memiliki antarmuka yang memungkinkan pengaturan firewall, pembagian bandwidth, serta pemantauan trafik jaringan secara langsung melalui aplikasi Winbox.

Tabel 1. Spesifikasi Mikrotik RouterBoard RB941-2nD

Product Code	RB941-2nD
Architecture	SMIPS
CPU	QCA9533
CPU core count	1
CPU nominal frequency	650 Mhz
Switch chip model	QCA9533-BL3A
RouterOS license	4
Operating system	RouterOS
Size of RAM	32 MB
Storage size	16 MB
Storage type	FLASH
MTBF	Approximately 100’000 hours at 25C
Tested ambient temperature	-20°C to 60°C

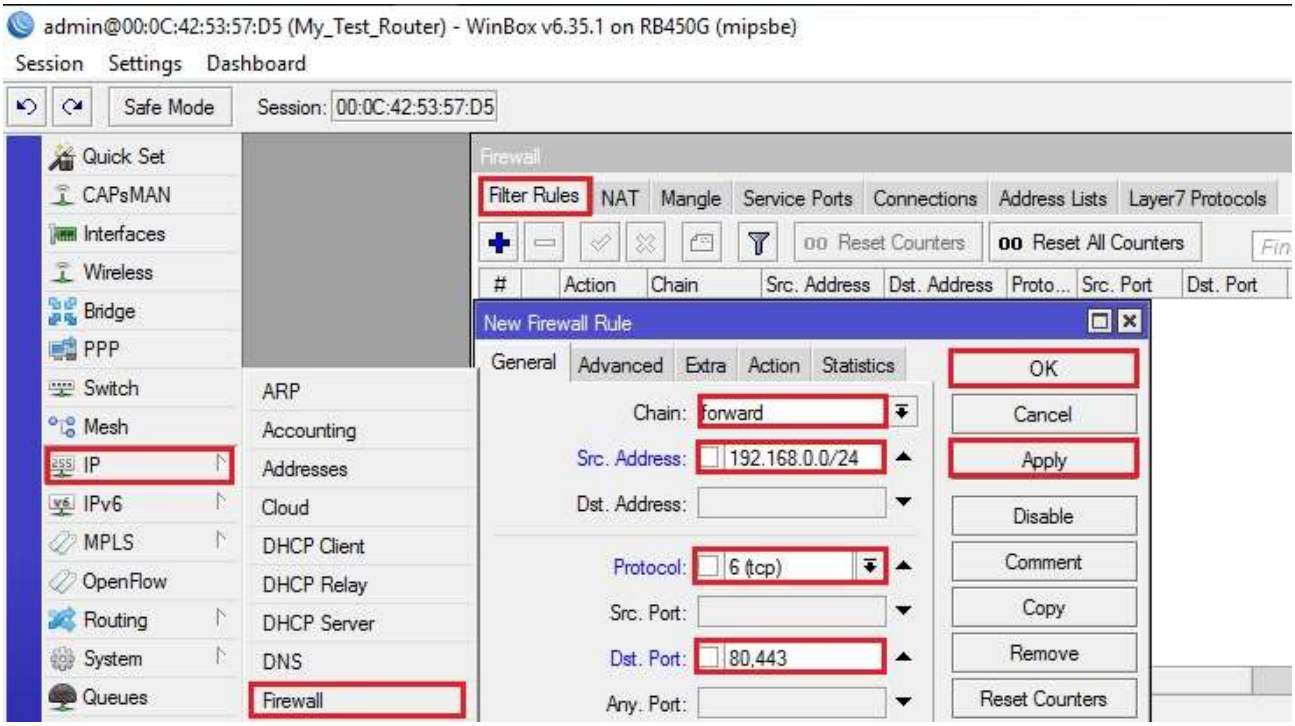
Setelah perangkat dipasang, administrator sekolah mulai melakukan pengaturan dasar agar semua komputer di jaringan mendapatkan alamat IP secara otomatis dan koneksi internet tersalurkan dengan lancar. Jalur utama dari modem ISP diarahkan ke router Mikrotik agar setiap koneksi internet melewati perangkat ini terlebih dahulu. Dengan sistem ini, setiap aktivitas jaringan dapat dikontrol dari satu titik pusat tanpa perlu melakukan konfigurasi pada setiap komputer.

Setelah seluruh perangkat berhasil terhubung melalui Mikrotik, jaringan sekolah menjadi lebih mudah dikelola. Administrator dapat memantau setiap koneksi dari laboratorium maupun ruang guru secara real-time melalui tampilan Winbox. Dari hasil observasi, koneksi antarperangkat menjadi lebih stabil dibanding sebelum penerapan firewall. Selain itu, sekolah kini memiliki kendali penuh terhadap distribusi internet tanpa perlu menambah perangkat tambahan. Tahapan ini menjadi dasar dari keseluruhan sistem keamanan jaringan di sekolah. Setelah jaringan terpusat melalui Mikrotik, tahap berikutnya adalah penerapan Layer 7 Protocol untuk melakukan pembatasan akses ke situs yang tidak mendukung kegiatan belajar. Langkah ini diterapkan pada konfigurasi berikutnya agar fungsi firewall tidak hanya mengatur koneksi, tetapi juga mampu menyaring konten berdasarkan kebutuhan sekolah.

3.2 Penerapan Layer 7 Protocol Untuk Penyaringan Situs Non-Pembelajaran

Tahap selanjutnya setelah sistem firewall terpasang dengan baik adalah penerapan fitur penyaringan berbasis Layer 7 Protocol. Langkah ini dilakukan agar penggunaan internet di lingkungan sekolah lebih terarah pada kegiatan belajar, dengan membatasi akses ke situs hiburan dan media sosial. Proses penerapan dimulai dari pembuatan pola pencocokan (pattern matching) pada menu IP → Firewall → Layer7 Protocols di aplikasi Winbox.

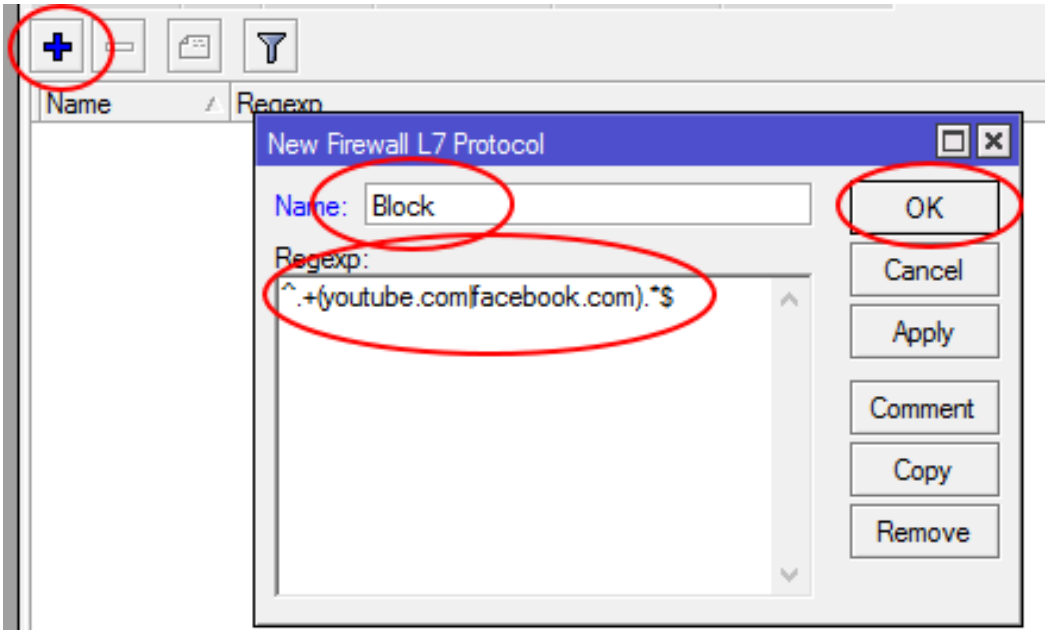
Dalam proses ini, administrator membuat daftar pola tertentu yang mewakili domain situs yang tidak diizinkan, seperti YouTube, TikTok, Facebook, dan platform hiburan lainnya. Setiap pola dibuat dengan menuliskan ekspresi karakter (regular expression) agar sistem dapat mengenali jenis trafik berdasarkan isi data yang lewat. Pola ini kemudian disimpan dan digunakan sebagai acuan dalam aturan pemblokiran.



Gambar 3. Pembuatan pola Layer 7 Protocol pada aplikasi Winbox

Setelah pola Layer 7 dibuat, tahap berikutnya adalah menambahkan aturan baru pada menu Filter Rules. Administrator menambahkan rule dengan mengarahkan chain pada bagian forward, memilih Layer7 Protocol sesuai nama pola yang sudah dibuat, lalu menentukan action dengan opsi drop. Dengan cara ini, setiap koneksi yang sesuai dengan pola tersebut akan langsung diblokir oleh firewall sebelum mencapai tujuan.

Selama proses penerapan, pengujian dilakukan menggunakan beberapa komputer di laboratorium sekolah. Administrator mencoba membuka berbagai situs hiburan untuk memastikan aturan berjalan dengan baik. Hasilnya menunjukkan bahwa semua situs yang masuk dalam pola Layer 7 tidak dapat diakses. Namun, situs pembelajaran tetap bisa dibuka tanpa hambatan.



Gambar 4. Contoh aturan firewall yang menggunakan Layer 7 Protocol dengan aksi pemblokiran

Tabel 2. Hasil penerapan aturan Layer 7 Protocol pada jaringan sekolah

Kategori Akses	Contoh Situs	Hasil Setelah Layer 7 Aktif
Hiburan	youtube.com	Terblokir
Media Sosial	facebook.com	Terblokir
Edukasi	classroom.google.com	Dapat diakses

Penerapan Layer 7 Protocol ini dilakukan dengan hati-hati agar tidak mengganggu akses ke situs yang mendukung kegiatan belajar. Sebelum aturan diberlakukan secara permanen, administrator melakukan beberapa kali penyesuaian pada pola teks agar hasil pemblokiran lebih akurat. Misalnya, beberapa situs pembelajaran menggunakan elemen dari domain video besar seperti ytimg.com, sehingga perlu dikecualikan agar tidak ikut diblokir.

Selama masa observasi, sistem Layer 7 berjalan dengan baik tanpa menimbulkan gangguan berarti pada koneksi internet. Aktivitas pembelajaran daring di laboratorium komputer berjalan lancar, dan bandwidth sekolah menjadi lebih terkendali karena trafik ke situs non-edukatif berhasil dikurangi.

Administrator juga melakukan pemantauan melalui menu Torch di Winbox untuk melihat arus koneksi secara langsung. Dari hasil pengamatan, trafik menuju situs-situs yang termasuk dalam pola Layer 7 menurun drastis, sementara akses ke situs pendidikan meningkat. Hasil ini menunjukkan bahwa penerapan Layer 7 tidak hanya membatasi akses, tetapi juga membantu menstabilkan koneksi di jam-jam padat.

Penerapan sistem ini membuat penggunaan internet di sekolah menjadi lebih terarah. Siswa tidak lagi dapat membuka situs hiburan, sementara guru dapat menjalankan pembelajaran daring tanpa gangguan. Tahapan ini juga membantu sekolah menghemat penggunaan bandwidth karena sebagian besar trafik non-pendidikan telah berhasil diblokir. Sistem firewall kini bekerja tidak hanya sebagai pengaman jaringan, tetapi juga sebagai alat pengatur perilaku digital di lingkungan pendidikan.

3.3 Implementasi Firewall di Lingkungan Madrasah Ibtidaiyah Fatahillah

Setelah proses konfigurasi selesai, tahap berikutnya adalah penerapan firewall secara menyeluruh di lingkungan Madrasah Ibtidaiyah Fatahillah. Penerapan dilakukan dengan menghubungkan seluruh perangkat komputer sekolah ke jaringan yang sudah melewati sistem Mikrotik. Koneksi utama berasal dari modem ISP, kemudian diarahkan ke Mikrotik RouterBoard RB941-2nD, sebelum akhirnya didistribusikan ke setiap ruangan melalui switch utama. Pada tahap ini, seluruh lalu lintas data sekolah sepenuhnya dikendalikan oleh Mikrotik.

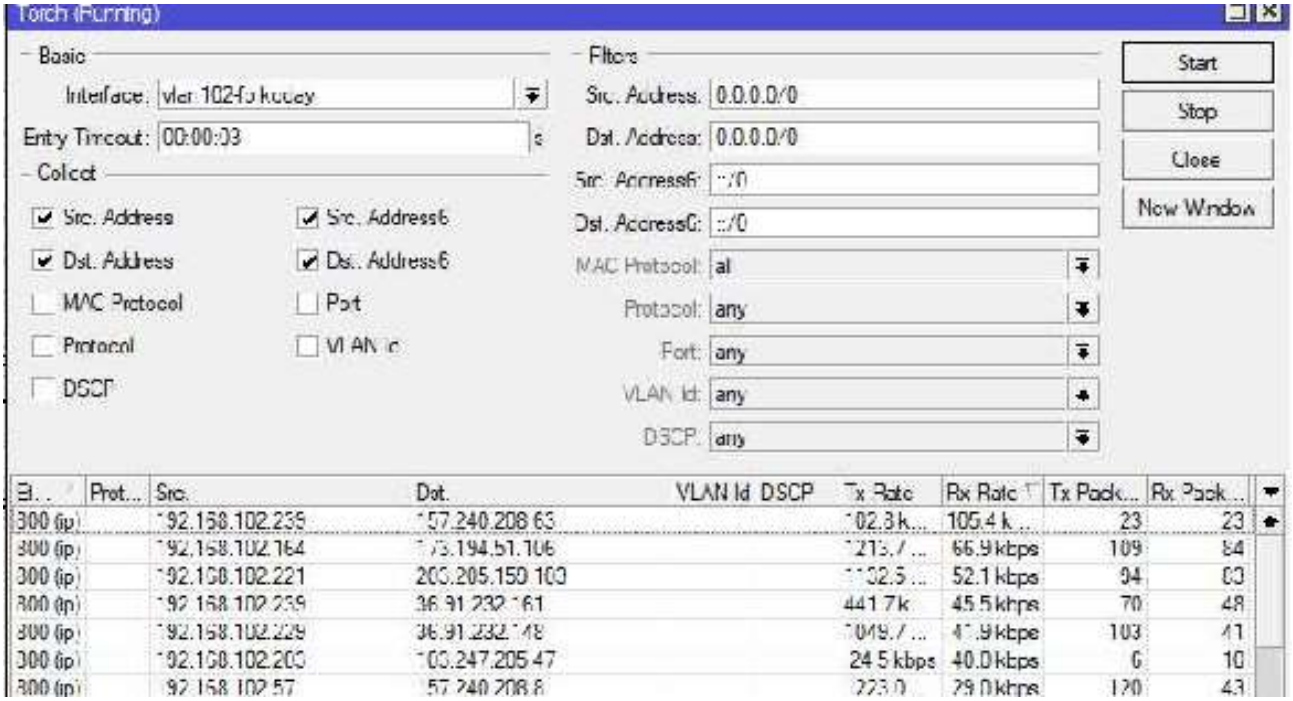
Penerapan dilakukan secara bertahap agar tidak mengganggu kegiatan belajar. Hari pertama difokuskan pada ruang guru, di mana dilakukan pengalihan koneksi dari router bawaan ISP ke Mikrotik. Setelah koneksi stabil, jaringan di laboratorium komputer mulai disesuaikan agar seluruh komputer siswa melewati firewall. Administrator juga memastikan setiap perangkat mendapatkan IP otomatis dari Mikrotik dan terdaftar di daftar leases DHCP agar mudah dimonitor.

Setelah semua ruangan terkoneksi melalui firewall, administrator melakukan pemantauan terhadap aktivitas jaringan melalui fitur Torch dan Traffic Monitor pada Winbox. Dari hasil pengamatan, terlihat bahwa lalu lintas internet kini mengalir terpusat melalui satu gateway, sehingga aktivitas penggunaan dapat dikontrol lebih mudah. Akses ke situs yang diblokir melalui Layer 7 tidak lagi dapat diakses dari komputer mana pun di jaringan sekolah.

Untuk memastikan firewall berfungsi optimal, administrator juga menambahkan beberapa aturan tambahan untuk membatasi port tertentu yang tidak digunakan dalam kegiatan pembelajaran. Dengan aturan tersebut, hanya koneksi penting seperti HTTP, HTTPS, dan DNS yang dibiarkan berjalan. Hal ini dilakukan untuk menjaga kestabilan bandwidth serta menghindari adanya perangkat asing yang mencoba mengakses jaringan sekolah.

Tabel 3. Kondisi jaringan sekolah

Ruang / Area	Jumlah Perangkat	Kondisi Setelah Implementasi Firewall
Laboratorium Komputer	20 unit	Akses internet stabil, situs non-edukatif diblokir
Ruang Guru	10 unit	Dapat mengakses situs administrasi dan pembelajaran
Ruang Kepala Sekolah	2 unit	Akses penuh dengan kontrol dari router
Area Umum (Wi-Fi)	5 perangkat	Terbatas hanya pada domain pendidikan
Total Jaringan Aktif	37 perangkat	Seluruhnya terhubung melalui Mikrotik



Gambar 5. Monitoring aktivitas jaringan menggunakan fitur Torch pada Mikrotik

Selama beberapa minggu setelah penerapan, koneksi jaringan di madrasah berjalan lebih stabil dan mudah dikontrol. Penggunaan bandwidth menjadi lebih efisien karena tidak ada lagi trafik dari situs-situs hiburan. Sementara itu, guru dan siswa dapat menggunakan internet dengan lebih fokus pada materi pembelajaran. Administrator juga mencatat bahwa jumlah keluhan terkait koneksi internet menurun cukup signifikan dibandingkan sebelum firewall diterapkan.

Kondisi ini menunjukkan bahwa penerapan firewall Mikrotik di lingkungan sekolah bukan hanya membantu dalam hal keamanan, tetapi juga mendukung efektivitas kegiatan belajar berbasis internet. Sistem yang sebelumnya terbuka kini menjadi lebih terarah dan aman. Firewall yang diterapkan juga memberi fleksibilitas kepada pihak sekolah untuk menambah atau menyesuaikan aturan sesuai kebutuhan di kemudian hari.

Torch (Running)

Basic

Interface: lanbridge

Entry Timeout: 00:00:03 s

Filters

Src. Address : 0.0.0.0/0

Dst. Address : 0.0.0.0/0

Src. Address6 : ::/0

Dst. Address6 : ::/0

MAC Protocol : all

Protocol : any

Port : any

VLAN Id : any

DSCP : any

Eth. P.../	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	192.168.20.71:60003	192.168.20.1:8291 (winbox)			699.9 k...	28.5 kbps	21	33
800 (ip)	17 (udp)	192.168.20.95:9500	184.72.173.0:9500			816 bps	1008 bps	1	1
800 (ip)	6 (tcp)	192.168.20.25:59996	216.239.36.131:5223			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.20.93:55893	52.6.79.234:443 (https)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.20.105:48218	96.113.17.239:11068			18.9 kbps	4.2 kbps	8	8
800 (ip)	17 (udp)	192.168.20.53:57691	52.96.79.178:443 (https)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.20.71:59621	151.101.128.176:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.53:62145	52.96.79.226:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.53:63211	52.96.156.2:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.53:53097	52.96.242.34:443 (https)			0 bps	0 bps	0	0
800 (ip)	1 (icmp)	192.168.20.53	52.96.242.34			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.185:40978	192.168.20.1:53 (dns)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.53:50426	52.96.79.178:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.53:58284	52.96.79.226:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.53:61445	52.96.156.2:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.53:60288	52.96.242.34:443 (https)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.20.71:64645	17.248.207.66:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.43:46384	192.168.20.1:53 (dns)			0 bps	0 bps	0	0
800 (ip)	1 (icmp)	192.168.20.43	75.2.70.75			0 bps	0 bps	0	0
800 (ip)	1 (icmp)	192.168.20.43	192.168.20.1			0 bps	0 bps	0	0
800 (ip)	1 (icmp)	192.168.20.43	192.168.20.1		48	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.20.71:59809	3.213.42.93:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	169.254.109.120:50760	239.255.255.250:1900			0 bps	0 bps	0	0
800 (ip)	17 (udp)	169.254.109.120:50759	239.255.255.250:1900			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.248:33242	255.255.255.255:10001			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.95:12027	44.206.234.216:9503			0 bps	54.5 kbps	0	5
800 (ip)	17 (udp)	192.168.20.71:23428	103.195.103.66:9993			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.71:9993	66.90.98.98:9993			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.71:23428	66.90.98.98:9993			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.71:23427	66.90.98.98:9993			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.71:9993	84.17.53.155:9993			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.71:23427	84.17.53.155:9993			0 bps	0 bps	0	0
800 (ip)	17 (udp)	192.168.20.71:23428	84.17.53.155:9993			0 bps	0 bps	0	0

Gambar 6. Tampilan distribusi koneksi jaringan setelah firewall aktif

Dari hasil observasi lapangan, implementasi firewall ini menjadi dasar utama bagi sekolah dalam mengelola jaringan yang lebih aman dan efisien. Setiap koneksi kini dapat dipantau secara real-time, dan akses internet di lingkungan sekolah berjalan sesuai dengan kebijakan yang telah ditentukan. Setelah tahap ini berhasil, kegiatan berikutnya adalah melakukan pengujian kinerja jaringan untuk menilai seberapa besar peningkatan kestabilan dan efisiensi yang dihasilkan dari sistem firewall yang diterapkan.

3.4 HASIL PENGUJIAN EFEKTIVITAS SISTEM FIREWALL MIKROTIK ROUTER OS

Tahap pengujian dilakukan setelah seluruh konfigurasi firewall dan fitur Layer 7 Protocol aktif di jaringan sekolah. Tujuan utama pengujian ini adalah menilai stabilitas koneksi, efektivitas penyaringan situs, serta efisiensi penggunaan bandwidth setelah sistem firewall diterapkan. Pengujian dilakukan selama satu minggu penuh pada jam operasional sekolah, dengan memantau lalu lintas data melalui aplikasi Winbox menggunakan fitur Torch, Traffic Monitor, dan Log Activity.

Pengujian awal dilakukan dengan mengukur kecepatan akses internet dari beberapa komputer di ruang guru dan laboratorium komputer. Sebelum sistem firewall diterapkan, kecepatan unduh sering kali menurun drastis saat jam sibuk. Setelah firewall aktif, koneksi menjadi lebih stabil karena seluruh trafik internet sudah dikendalikan oleh Mikrotik. Setiap koneksi menuju situs non-pembelajaran berhasil diblokir melalui aturan Layer 7 yang sudah diterapkan.



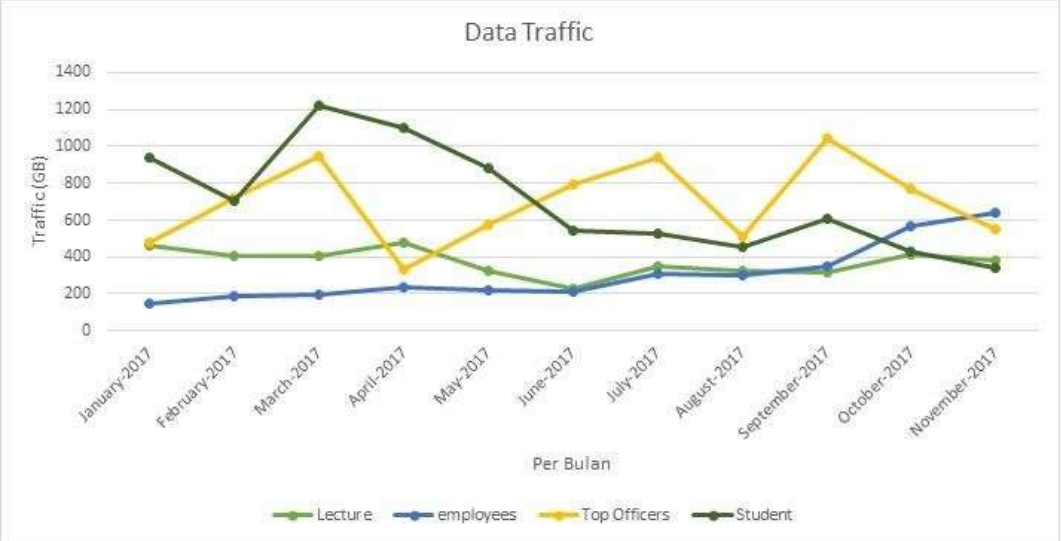
Gambar 7. Monitoring trafik jaringan setelah sistem firewall aktif

Berdasarkan hasil pengamatan, sistem firewall mampu menjaga kestabilan koneksi di semua ruangan. Trafik jaringan terlihat lebih terkendali karena hanya koneksi dengan protokol tertentu yang diizinkan. Administrator mencatat penurunan trafik non-edukatif secara signifikan setelah firewall dan Layer 7 Protocol diaktifkan. Selama masa uji, tidak ditemukan lagi lonjakan trafik dari situs hiburan, dan seluruh perangkat terpantau aktif dengan kecepatan yang seragam.

Untuk menilai efektivitas firewall, dilakukan perbandingan penggunaan bandwidth sebelum dan sesudah sistem berjalan. Hasilnya menunjukkan penurunan rata-rata konsumsi bandwidth harian sebesar 30–40%. Bandwidth yang sebelumnya terserap oleh situs hiburan kini dapat digunakan sepenuhnya untuk kegiatan pembelajaran daring. Selain itu, sistem rule hit counter pada Mikrotik menunjukkan jumlah pemblokiran yang tinggi pada kategori situs non-edukatif, menandakan bahwa mekanisme filter berfungsi dengan baik.



Gambar 8. Efektivitas firewall Mikrotik dalam mengurangi bandwidth non-edukatif



Gambar 9. Perbandingan trafik edukasi dan non-edukasi setelah penerapan firewall

Hasil pengamatan pada gambar di atas menunjukkan adanya pergeseran pola penggunaan internet yang cukup jelas. Setelah penerapan firewall, trafik menuju situs Pendidikan meningkat hingga dua kali lipat, sementara trafik ke situs hiburan turun drastis. Kondisi ini menunjukkan bahwa firewall tidak hanya menjaga keamanan jaringan, tetapi juga berhasil mengarahkan perilaku penggunaan internet menjadi lebih produktif dan sesuai dengan tujuan pembelajaran.

Dari keseluruhan hasil uji, dapat disimpulkan bahwa penerapan firewall Mikrotik RouterOS di Madrasah Ibtidaiyah Fatahillah berjalan efektif dan memberikan dampak positif pada kestabilan jaringan, efisiensi bandwidth, serta pengendalian akses pengguna. Sistem ini mampu meminimalkan risiko kebocoran data, mencegah akses konten yang tidak sesuai, dan mendukung terciptanya lingkungan digital yang aman serta kondusif bagi kegiatan belajar mengajar.

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa penggunaan perangkat Mikrotik RouterBoard RB941-2nD mampu menjalankan fungsi pengendalian jaringan secara optimal di lingkungan Madrasah Ibtidaiyah Fatahillah. Penerapan Layer 7 Protocol efektif dalam menyaring dan memblokir akses ke situs yang tidak relevan dengan kegiatan pembelajaran, sehingga penggunaan internet menjadi lebih terarah. Implementasi yang dilakukan pada jaringan sekolah terbukti berjalan stabil dan tidak menimbulkan gangguan terhadap akses layanan edukatif yang diperlukan. Hasil pengujian juga memperlihatkan bahwa konfigurasi firewall yang diterapkan mampu meningkatkan keamanan jaringan, mengurangi trafik non-produktif, serta memberikan efisiensi penggunaan bandwidth secara signifikan, sehingga keseluruhan sistem jaringan sekolah menjadi lebih aman, terkendali, dan mendukung proses pembelajaran dengan baik.

REFERENSI

[1] D. W. Adi, Z. R. Athallah, F. Irawan, and S. N. Neyman, "Implementasi Firewall menggunakan Fitur dari IPTables pada Sistem Operasi Linux," J. Internet Softw. Eng., vol. 1, no. 2, p. 7, 2024, doi: 10.47134/pjise.v1i2.2671.

[2] N. A. Sagala, H. Jusuf, G. C. Lestari, A. Wasid, and D. Irawan, "Implementasi Keamanan Jaringan dan Filtering Web Server Menggunakan pfSense Pada PT.Televisi Transformasi Indonesia," J. Inform. dan Komputasi Media Bahasan, Anal. dan Apl., vol. 18, no. 2, pp. 67–71, 2024, doi: 10.56956/jiki.v18i2.370.

[3] H. A. Al Kautsar and R. Sastra, "Implementasi Firewall Mikrotik dalam Pembatasan Akses Situs Terlarang di RT/RW Net," Comput. Sci., vol. 5, no. 2, pp. 123–132, 2025, doi: 10.31294/coscience.v5i2.8897.

[4] A. B. Rifai, M. Tahir, V. S. Pramesta, W. P. Sari, and R. Harnindia, "Implementasi Manajemen Hotspot dan Sistem Keamanan Jaringan Menggunakan Mikrotik dengan Metode Firewall Layer 7 Protocol di SMPN 1 Balong Panggang," vol. 7, no. 3, pp. 215–221, 2024.

[5] C. N. Syahputri, C. Anggraini, H. F. Anugerah, I. Zufria, and M. I. Nahwi, "Penerapan Kinerja Filter Rule dengan Metode Raw dan Layer 7 Protocol di Router Mikrotik," J. Kridatama Sains Dan Teknol., vol. 5, no. 02, pp. 433–447, 2023, doi: 10.53863/kst.v5i02.969.

[6] I. Kumalasari and A. Yadi Saputra, "Implementasi Malware Security and Proxy Layer 7 Protocol at Routerboard Mikrotik," bit-Tech, vol. 5, no. 2, pp. 128–135, 2022, doi: 10.32877/bt.v5i2.953.

[7] Y. Sianhar and M. Marhalim, "Penerapan Firewall Berbasis Mikrotik Dalam Optimalisasi Jaringan Di Sekolah Menengah Kejuruan," J. Inform. Teknol. dan Sains, vol. 7, no. 2, pp. 868–877, 2025, doi: 10.51401/jinteks.v7i2.5774.

[8] H. Aswad, Y. Akbar, M. U. H. Asrori, and F. Toriq, "Pengembangan Sistem Firewall Adaptif Berbasis DNS untuk Memblokir Situs Pornografi di Jaringan IDN Boarding School," (Jurnal Teknol. Inf. dan Komunikasi), vol. 9, no. September, pp. 1166–1174, 2025.

[9] W. Styorini, H. Azwar, and Mochammad Susantok, "Implementasi Firewall Pada Laboratorium Jaringan Komputer SMAIT AL-ITTIHAD," JITER-PM (Jurnal Inov. Terap. - Pengabdi. Masyarakat), vol. 2, no. 1, pp. 38–44, 2024, doi: 10.35143/jiter-pm.v2i1.6162.