IMPLEMENTASI *FIREWALL* DAN *FILTERING FIREWALL* BERBASIS MIKROTIK DENGAN METODE *LAYER7 PROTOCOL* DI SMK AL - HIKAM

Raja Gafira Wirdana Zain, Muhlis Tahir, Alvienda Ricka Seviana, Camelia Savitri, Wilda Nur Mei Syahrina, Alfian Andika El-faizi
Program Studi Pendidikan Informatika, Universitas Trunojoyo Madura
Jl. Raya Telang, Kec. Kamal, Kab. Bangkalan
rajagafira47@gmail.com

ABSTRAK

Kemajuan teknologi informasi memberikan dampak signifikan terhadap dunia pendidikan, salah satunya melalui penyediaan akses internet di lingkungan sekolah. Namun, akses internet yang tidak terkontrol dapat menimbulkan permasalahan serius, seperti siswa mengakses situs-situs yang tidak sesuai dengan tujuan pembelajaran, termasuk media sosial. SMK Al-Hikam mengalami permasalahan serupa, sehingga diperlukan solusi untuk mengendalikan dan memfilter lalu lintas internet yang digunakan oleh siswa. Penelitian ini bertujuan untuk mengimplementasikan sistem *firewall* berbasis MikroTik menggunakan metode *Layer7 Protocol* sebagai upaya menyaring konten-konten yang tidak diinginkan. Metode yang digunakan meliputi observasi dan wawancara dengan pihak sekolah untuk menggali kebutuhan sistem keamanan jaringan, serta implementasi konfigurasi *firewall* melalui perangkat lunak VirtualBox, aplikasi Winbox, dan pengaturan *Layer7 Protocol*, Filter Rules, dan NAT Rule pada router MikroTik. Pengujian dilakukan dengan mengakses berbagai situs terlarang setelah konfigurasi diterapkan. Hasil penelitian menunjukkan bahwa sistem *firewall* yang dikembangkan mampu secara efektif memblokir akses ke situs media sosial seperti Facebook, Instagram, Tiktok, sehingga tercipta lingkungan pembelajaran yang lebih aman, kondusif, dan mendukung kegiatan belajar mengajar di SMK Al-Hikam. Berdasarkan hasil tersebut, disarankan melakukan pemeliharaan rutin serta memberikan edukasi kepada siswa mengenai etika penggunaan internet untuk menjaga keberlangsungan sistem yang telah dibangun.

Kata kunci : *Mikrotik, Layer7 Protocol, Firewall, Filtering, Keamanan Jaringan, SMK Al - Hikam*

1. PENDAHULUAN

Perkembangan teknologi dan komunikasi yang pesat berperan penting dalam berbagai aspek kehidupan, termasuk ekonomi, kesehatan, dan pendidikan. Internet menjadi sumber informasi yang paling cepat dan efektif. Seiring dengan meningkatnya jumlah pengguna, kebutuhan akan jaringan yang lebih efisien dan aman semakin meningkat [1]. Begitu juga dengan komunikasi data, mulai dari koneksi antar dua komputer hingga jaringan komputer. Jaringan komputer saat ini merupakan suatu layanan yang sangat dibutuhkan. Jaringan komputer mempunyai manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri. Jaringan komputer memungkinkan pemakaian secara bersama data, perangkat lunak dan peralatan. Sehingga kelompok kerja dapat berkomunikasi lebih efektif dan efisien Hal ini mendorong institusi, baik pemerintah maupun swasta, untuk mengimplementasikan sistem keamanan yang handal guna melindungi data dan informasi yang sensitif [2].

Peran jaringan di berbagai aspek konektivitas sangat membantu untuk proses berjalannya hubungan komunikasi antara satu sama lain, sehingga banyak yang beralih dari manual menggunakan jaringan komputer. Tetapi pada jaringan komputer tentunya dibutuhkan beberapa management untuk merawat dan melindungi data agar tidak bocor keluar, dalam hal ini perusahaan harus benar-benar serius agar jaringan komputer di perusahaan tersebut tidak mudah di retas dari dalam maupun dari luar. Selain melindungi dari ancaman *Cyber Crime* Menurut Krianto Sulaiman (2016), Salah satu factor yang mempengaruhi kualitas dalam jaringan adalah *network security* atau keamanan jaringan, banyak teknik yang dapat dilakukan dalam meningkatkan keamanan jaringan, baik dengan membangun *system firewall*, dengan menggunakan *layer7 protocol* maupun dengan *port security*, *port security* memanfaatkan *port-port* yang ada untuk mengizinkan akses ke jaringan. [3]. Keamanan jaringan sebagai aspek krusial dalam melindungi data sensitif, sehingga diperlukan berbagai metode untuk mengantisipasi ancaman terhadap infrastruktur jaringan [4].

Di lingkungan pendidikan, seperti di SMK Al Hikam, akses internet yang tidak terkontrol dapat menimbulkan dampak negatif bagi siswa. Konten-konten berbahaya seperti pornografi, *cyberbullying*, dan informasi yang tidak sesuai dapat dengan mudah diakses oleh siswa, sehingga membahayakan proses belajar mengajar dan perkembangan mental mereka. Oleh karena itu, penerapan *firewall* dan *filtering content* menjadi sangat penting. Melalui penggunaan MikroTik sebagai alat untuk membangun *firewall*, sekolah dapat memblokir akses ke situs-situs yang tidak diinginkan dan mengatur penggunaan internet menjadi lebih produktif dan aman bagi siswa [5]. Implementasi *firewall* adalah solusi perlindungan penting dalam jaringan komputer yang berfungsi untuk mencegah serangan dan penyusupan yang dapat membahayakan kerahasiaan data serta merusak infrastruktur jaringan [6].

Sebelum penelitian ini dilakukan, siswa SMK AL - Hikam menggunakan akses internet dengan bebas mengakses situs yang tidak mendukung kegiatan belajar seperti situs Instagram, facebook, dan tiktok. Dengan tidak adanya *filtering* jaringan hal-hal yang tidak mendukung kegiatan belajar sering terjadi dilingkungan sekolah dan tentunya kurang efektif dalam penggunaan internet karena pengguna internet di lingkungan sekolah tidak terkontrol disebabkan oleh bebasnya pengguna internet untuk mengakses dengan menggunakan internet yang tersedia di sekolah.

Berdasarkan permasalahan tersebut penelitian ini bertujuan untuk melakukan implementasi *firewall* menggunakan mikrotik dengan metode *layer7 protocol* di SMK AL - HIKAM. Dengan menerapkan *firewall* yang tepat, diharapkan para siswa dapat menggunakan komputer secara bijak untuk kepentingan pendidikan, sekaligus memblokir akses ke situs-situs yang tidak diinginkan. Konfigurasi *firewall* ini penting untuk menjaga agar jaringan tetap aman dan terhindar dari konten yang dapat merusak mental dan moral siswa.

2. TINJAUAN PUSTAKA

Penelitian mengenai implementasi *firewall* dan *filtering firewall* pada Mikrotik dalam upaya mengoptimalkan keamanan jaringan di SMK Al - Hikam bertujuan untuk meningkatkan perlindungan jaringan melalui pengelolaan akses internet. Dengan memanfaatkan fitur *Layer7 Protocol* pada Mikrotik, diharapkan lalu lintas data yang melewati jaringan dapat dikontrol dan difilter secara efektif, sehingga mampu mengurangi risiko serangan siber serta penyalahgunaan akses internet oleh pengguna.

2.1. *Virtual Box*

Sebuah perangkat lunak virtual yang digunakan untuk menjalankan sistem operasi utama. Berfungsi sebagai virtualisasi sistem operasi, *virtual box* juga dapat dijadikan virtualisasi tambahan untuk jaringan komputer sederhana [1].

2.2. Mikrotik

Mikrotik *Routerboard* adalah perangkat jaringan yang diproduksi oleh Mikrotik, dirancang khusus untuk menjalankan fungsi *router network,* dan dilengkapi dengan sistem operasi bernama *RouterOS*. Perangkat ini beroperasi mirip dengan komputer, memiliki mainboard dengan *processor,* RAM, ROM, dan memori *flash*. Biasanya dalam melakukan konfigurasi mikrotik akan menggunakan aplikasi *Winbox*. Oleh karena itu, perangkat ini dapat beroperasi secara mandiri tanpa ketergantungan pada komputer yang berfungsi sebagai *server* [7].

2.3. *Winbox*

Winbox adalah sebuah utility yang dapat digunakan untuk melakukan remote ke server mikrotik dalam mode GUI. Jika untuk mengkonfigurasi mikrotik dalam text mode melalui PC itu sendiri, maka untuk GUI yang menggunakan winbox kita perlu mengkonfigurasi mikrotik melalui komputer clint Mengkonfigurasi mikrotik melalui winbox ini lebih banyak digunakan karena selain penggunaannya yang mudah, juga tidak harus menghafal perintah - perintah consule [8].

2.4. Keamanan Jaringan

Keamanan jaringan adalah proses untuk melindungi sistem dalam jaringan dengan mendeteksi penggunaan yang berhak dalam jaringan. Pengelolahan terhadap pengendalian keamanan jaringan dapat dilihat dari sisi pengelolahan resiko (*Risk Management*). *Wireless Intrusion Detection System* (WIDS) dapat didefinisikan sebagai *tools*, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktifitas jaringan komputer. *Wireless Intrusion Detection System* secara khusus berfungsi sebagai proteksi secara keseluruhan dari sistem yang telah di *install* WIDS. WIDS tidak berdiri sendiri dalam melindungi suatu sistem. Selain WIDS, juga terdapat *system* keamanan yang lain seperti *Intrusion Prevention System* (IPS), namun sistem ini hanya menggunakan parameter penyebaran inline atau satu jalur dan ketika mendeteksi potensi ancaman pengiriman peringatan sifatnya opsional sehingga bisa saja terjadi ancaman tapi tidak ada peringatan dari sistem. Sedangkan WIDS parameter penyebarannya melalui *spanning port* atau *network tap* dan Ketika mendeteksi ancaman, peringatan akan secara otomatis terkirim [9].

2.5. *Firewall*

Firewall adalah teknologi keamanan siber yang digunakan untuk meningkatkan keamanan komputer yang terhubung ke jaringan, seperti Jaringan Area Lokal (LAN) atau Internet. *Firewall* atau dalam Bahasa Indonesia diartikan sebagai Dinding Api adalah alat yang dapat mengurangi lubang keamanan dalam suatu organisasi komputer. Perancangan yang dibuat bisa memenuhi standar kerangka kerja, terutama dalam pembatasan penggunaan kuota data, serta dapat digunakan untuk menyaring informasi yang masuk melalui router. *Firewall* telah terbukti dapat melindungi jaringan dengan menyaring data secara selektif untuk meningkatkan kinerja *system* [10].

2.6. *Layer7 Protocol*

Layer7 Protocol adalah layer aplikasi yang berfungsi sebagai antarmuka aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS. *Layer7 Protocol* juga memiliki fungsi seperti memblokir sebuah situs dengan menambah filter rules baru. *Firewall* RAW merupakan salah satu fitur pada mikrotik yang bisa digunakan untuk bypass atau drop paket sebelum connection tracking. Dengan penerapan metode raw

firewall menghasilkan beberapa keuntungan diantaranya menghemat penggunaan sumber daya, hal ini dikarenakan raw memungkinkan melakukan connection tracking, sebelum memilih antara melewatkan atau memblokir packet [11].

2.7. Penelitian Terkait

Penelitian sebelumnya telah menunjukkan efektivitas penggunaan *Layer7 Protocol* dan *firewall* dalam meningkatkan keamanan jaringan. Sebuah penelitian yang dilakukan pada kelurahan Buaran Indah berhasil menerapkan *Firewall Layer7 Protocol* dengan mikrotik pada jaringan komputer kelurahan Buaran Indah staf maupun karyawan dapat menggunakan internet dengan stabil serta dapan dengan bijak menggunakan hak akses internet pada jam kerja dengan sebagaimana mestinya [1]. Penelitian lain menyimpulkan bahwa MikroTik efektif dalam mengatur dan mengamankan jaringan. MikroTik memungkinkan pembagian bandwidth teratur untuk setiap klien, penutupan port yang terbuka, pemblokiran akses ke situs web tertentu, dan kontrol jaringan melalui aplikasi WinBox. Dengan demikian, MikroTik memberikan solusi yang efisien dan aman untuk pengelolaan jaringan nirkabel, memastikan gangguan pada satu klien tidak mempengaruhi yang lain dan memberikan kontrol penuh kepada administrator [6].

Berdasarkan temuan dari penelitian sebelumnya, penelitian ini bertujuan untuk menerapkan *Layer7 Protocol* pada Mikrotik guna mengoptimalkan keamanan jaringan di SMK Al - Hikam. Penerapan ini diharapkan dapat meningkatkan kendali terhadap lalu lintas jaringan, membatasi akses ke konten yang tidak relevan, serta mengoptimalkan kinerja jaringan melalui sistem caching dan *filtering*.

3. METODE PENELITIAN

Dalam studi ini, perancangan yang diterapkan difokuskan pada upaya meningkatkan sistem jaringan komputer yang sudah ada dengan memanfaatkan fitur *content filtering* pada *Layer7 Protocol*. Penerapan ini bertujuan untuk mengendalikan akses internet siswa guna mencegah siswa mengunjungi situs yang tidak selaras dengan lingkungan pendidikan, seperti perjudian online, konten dewasa, serta laman lain yang tidak mendukung proses pembelajaran.

Guna mencapai tujuan tersebut, penelitian ini mengadopsi beberapa metode, yaitu:

a. Metode Observasi
   Pengambilan data dilakukan dengan cara mengamati secara langsung infrastruktur jaringan komputer di SMK Al-Hikam, yang beralamat di Jl. Raya Perum Tonjung No.01, Perumnas, Tunjung, Kec. Burneh, Kabupaten Bangkalan, Jawa Timur 69121. Observasi ini bertujuan untuk mendapatkan pemahaman yang lebih mendalam terkait sistem jaringan yang sedang digunakan serta potensi risiko keamanan yang dapat timbul.
b. Metode Wawancara
   Guna memperluas informasi yang telah dikumpulkan, wawancara dilakukan dengan Bapak Syamsul Ma'arif, sebagai guru yang mengajar mata pelajaran Teknologi Layanan Jaringan dan menjabat sebagai Staff IT di Bidang Teknik Komputer dan Jaringan di SMK Al - Hikam. Wawancara ini bertujuan untuk memperoleh pemahaman mengenai pengelolaan jaringan komputer, tantangan yang dihadapi, serta strategi yang diterapkan dalam meningkatkan keamanan jaringan.
c. Metode Studi Kepustakaan
   Penelitian ini juga mencakup kajian literatur dengan meneliti berbagai sumber, termasuk jurnal ilmiah, artikel, buku, serta referensi digital yang berkaitan. Studi pustaka ini bertujuan untuk memperkaya landasan teori dan dijadikan acuan dalam implementasi *Layer7 Protocol* pada jaringan sekolah.
d. Penerapan
   Tahap penerapan, yakni menjalankan konfigurasi agar sistem web filtering firewall dapat diterapkan. Proses dimulai dengan konfigurasi router mikrotik, di mana daftar situs yang perlu diblokir dimasukkan ke dalam sistem. Selanjutnya, aturan pemfilteran diaktifkan untuk membatasi akses ke situs-situs yang dianggap tidak kegiatan, seperti situs pornografi, judi online, dan game online.
e. Pengujian
   Tahap ini bertujuan untuk menguji mikrotik yang telah dikonfigurasi untuk memastikan sistem berfungsi dengan baik dan sesuai dengan standar kebutuhan.

4. HASIL DAN PEMBAHASAN

Dalam penelitian yang telah dilaksanakan di SMK Al - Hikam dengan menerapkan berbagai metode, diperoleh hasil sebagai berikut:

a. Informasi spesifik mengenai perangkat jaringan yang digunakan di SMK Al - Hikam tidak tersedia untuk publik. Namun, secara umum, sekolah tersebut memanfaatkan berbagai perangkat jaringan guna mendukung aktivitas pembelajaran dan operasional. Perangkat yang digunakan mencakup *router*, *switch*, *access point*, kabel jaringan, serta perangkat lunak manajemen jaringan seperti Mikrotik.
b. Akses internet di lingkungan sekolah diberikan kepada siswa serta staf pengajar dengan tujuan utama mendukung kegiatan pembelajaran dan administrasi.
c. Penyediaan fasilitas internet bagi siswa di SMK Al – Hikam (atau sekolah pada umumnya) bertujuan untuk menunjang proses pembelajaran dan pengembangan keterampilan teknologi. Selain itu, internet juga dimanfaatkan untuk mengakses sumber belajar, meningkatkan keterampilan teknologi, mendukung pembelajaran jarak jauh, mendorong penelitian

dan kewirausahaan, serta memperkuat kolaborasi dan komunikasi.

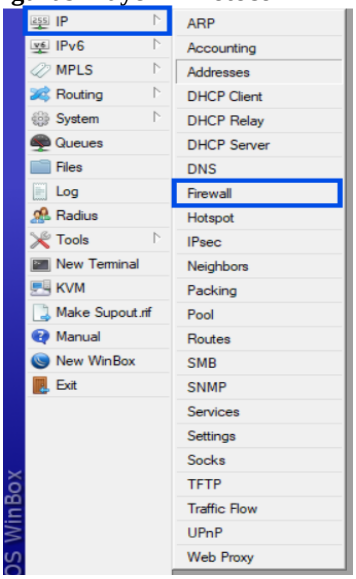
d. Terdapat indikasi adanya penyalahgunaan akses internet di SMK Al - Hikam, meskipun tidak terdapat informasi spesifik mengenai kasus yang terjadi di sekolah tersebut. Secara umum, bentuk-bentuk penyalahgunaan yang sering ditemukan di lingkungan sekolah mencakup akses ke konten yang tidak pantas, penggunaan internet untuk kepentingan pribadi, serta penyebaran konten yang tidak etis.
e. Beberapa langkah diterapkan untuk memastikan akses internet dimanfaatkan secara efektif dan sesuai dengan tujuan pembelajaran, salah satunya adalah sistem login dan password. Setiap siswa serta staf pengajar diberikan akun khusus yang digunakan untuk mengakses jaringan internet sekolah. Sistem autentikasi ini bertujuan memastikan bahwa hanya pengguna terdaftar yang dapat memanfaatkan akses internet di lingkungan sekolah.

Penelitian ini menekankan bahwa sistem jaringan komputer di SMK Al - Hikam masih belum maksimal dalam melakukan penyaringan terhadap konten negatif yang tidak mendukung aktivitas belajar siswa. Oleh karena itu, peneliti mengajukan penambahan konfigurasi pada Mikrotik untuk meningkatkan keamanan jaringan, terutama dalam memfilter konten yang kurang bermanfaat. Dengan langkah ini, siswa dapat memanfaatkan internet secara lebih bijaksana dan menunjang proses pembelajaran mereka.

4.1. Konfigurasi Usulan

Penulis membuat simulasi dengan menggunakan *VirtualBox* yang telah dikonfigurasi dengan Mikrotik *RouterOS*, sedangkan *Windows 11* berperan sebagai *client* dalam rancangan konfigurasi yang diajukan.

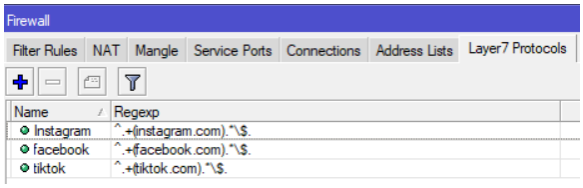
4.2. Konfigurasi Layer 7 Protocol



Gambar 1. Tampilan Menu *Firewall* di Mikrotik

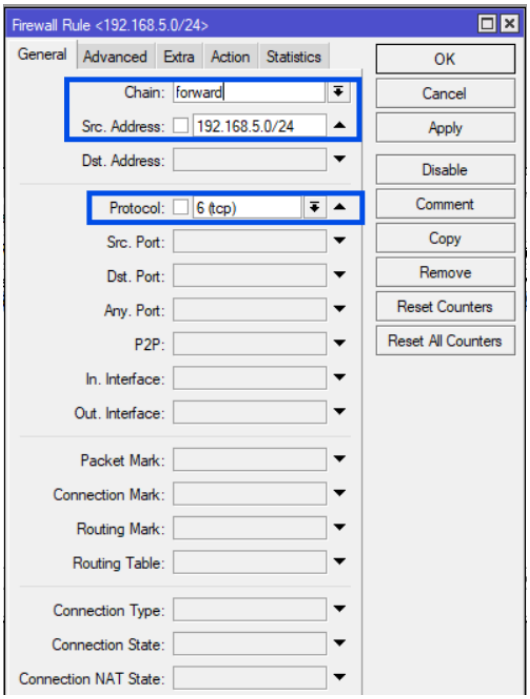
Konfigurasi *layer 7 protocol* dibutuhkan untuk membatasi akses user untuk mengakses ke konten tertentu atau *website* tertentu. Proses konfigurasi melibatkan Langkah-langkah berikut: Pertama, membuka aplikasi winbox dan melakukan koneksi ke perangkat Mikrotik secara remote. Kemudian, mengaktifkan *firewall* melalui menu panel disebelah kiri, dengan cara membuka IP kemudian *firewall*, seperti gambar 1.

Langkah selanjutnya adalah konfigurasi *layer7 protocol*, "*Blok Website*" merupakan nama untuk konfigurasi ini yang berisi *Regexp* yang berfungsi untuk memblokir beberapa situs web. Tampilan konfigurasi pada gambar 2.

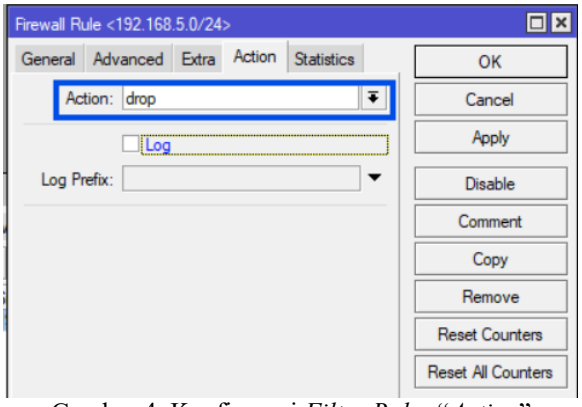


Gambar 2. Tampilan Konfigurasi *Layer7 Protocol*

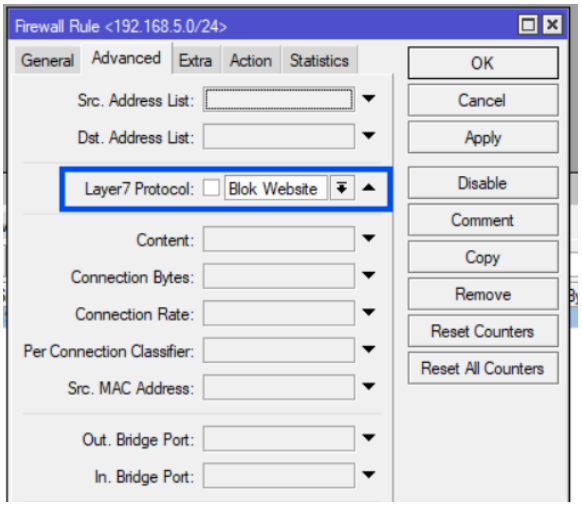
Langkah selanjutnya adalah konfigurasi "*Filter Rules*" konfigurasi action drop berfungsi untuk membatasi akses ke situs web tertentu, *chain forward* digunakan untuk memfilter paket data yang melewati *router*, *src. Address* atau alamat IP yang melakukan koneksi disini menggunakan IP 192.168.5.0/24, kemudian *protocol* 6 (tcp) untuk memastikan komunikasi yang sesuai dengan standar jaringan, dan pada menu *advanced* akan otomatis menggunakan konfigurasi *layer7 protocol* yang sudah di konfigurasi diawal. Tampilan *konfigurasi filter rules* seperti gambar berikut.



Gambar 3. Konfigurasi *Filter Rules* "*General*"

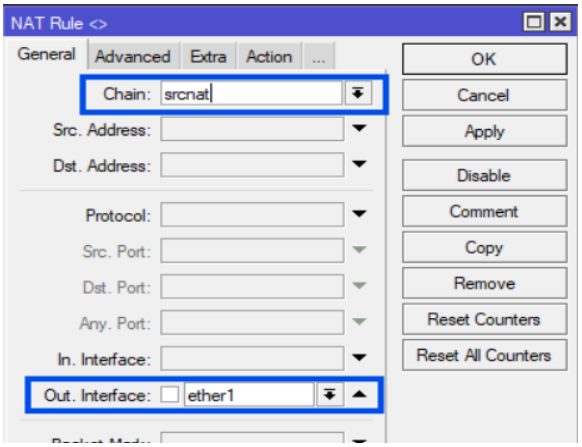


Gambar 4. Konfigurasi *Filter Rules* "*Action*"

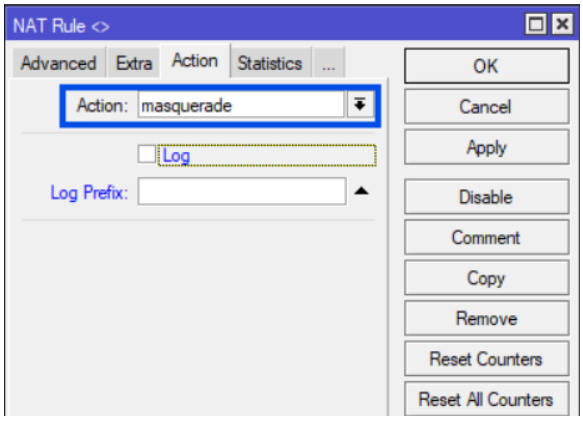


Gambar 5. Tampilan Konfigurasi *Filter Rules* "*Advanced*"

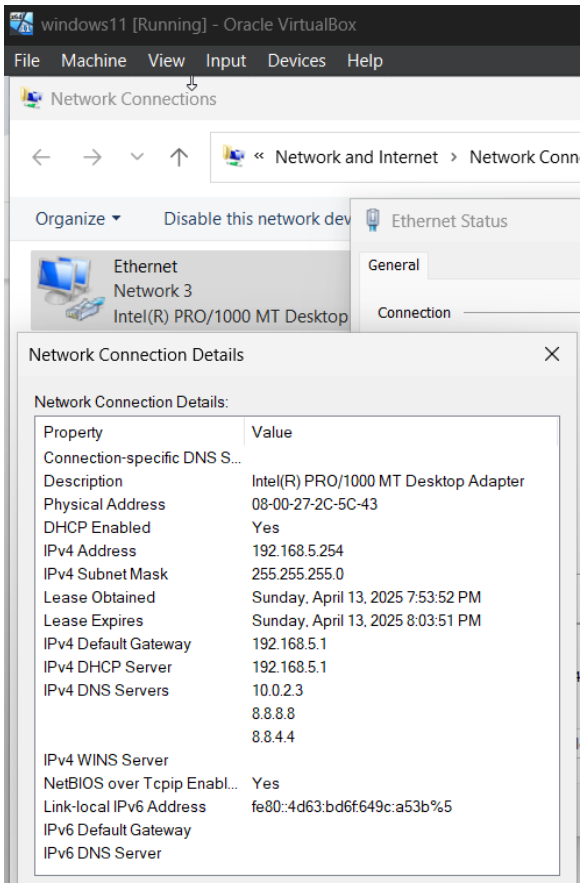
Langkah berikutnya konfigurasi NAT Rule, pada menu general kemudian chain "*srcnat*" berfungsi untuk mengubah IP local menjadi IP public, kemudian Out. Interface "*ether1*" berfungsi untuk mencari pola dalam aliran ICMP/TCP/UDP. Pada menu action "*masquerade*" berfungsi untuk menyembunyikan alamat IP komputer pribadi. Tampilan konfigurasi NAT *Rule* seperti gambar berikut.



Gambar 6. Tampilan Konfigurasi NAT *Rule* "*General*"



Gambar 7. Tampilan Konfigurasi NAT *Rule* "*Action*"

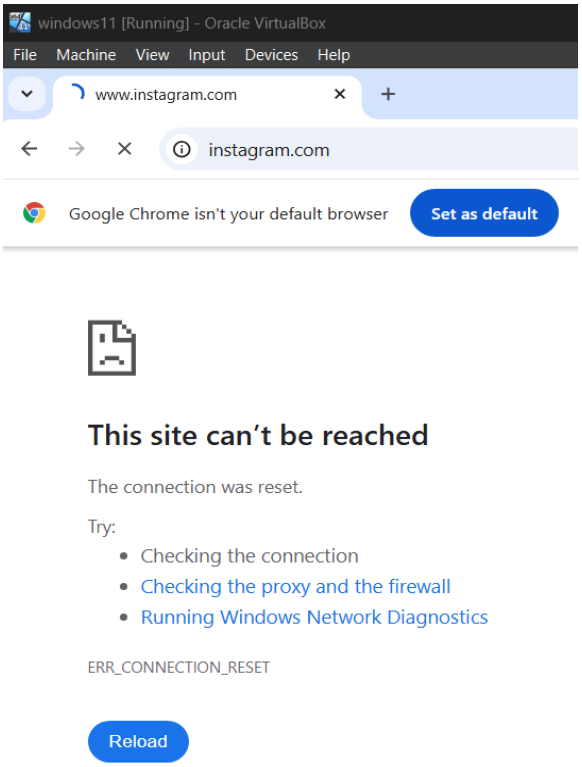


Gambar 8. Tampilan IP Client Setelah Selesai Konfigurasi di Mikrotik

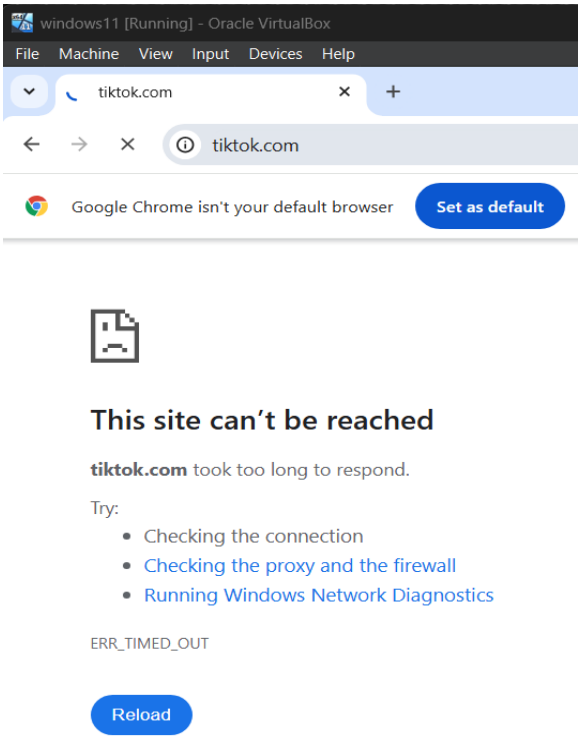
4.3. Pengujian

Setelah seluruh konfigurasi telah selesai dilakukan dengan benar, Langkah berikutnya adalah menguji efektivitas pengaturan yang telah diterapkan. Untuk melakukan pengujian, buka peramban web dan coba akses situs web yang sebelumnya telah dibatasi melalui konfigurasi *later7 protocol*. Jika situs web tersebut masih dapat diakses tanpa kendala, hal ini menandakan bahwa terdapat kesalahan dalam proses konfigurasi yang perlu diperiksa dan diperbaiki. Namun jika halaman situs web tidak dapat di akses maka dapar disimpulkan bahwa proses pemblokiran telah berhasil diterapkan dengan baik. Langkah ini

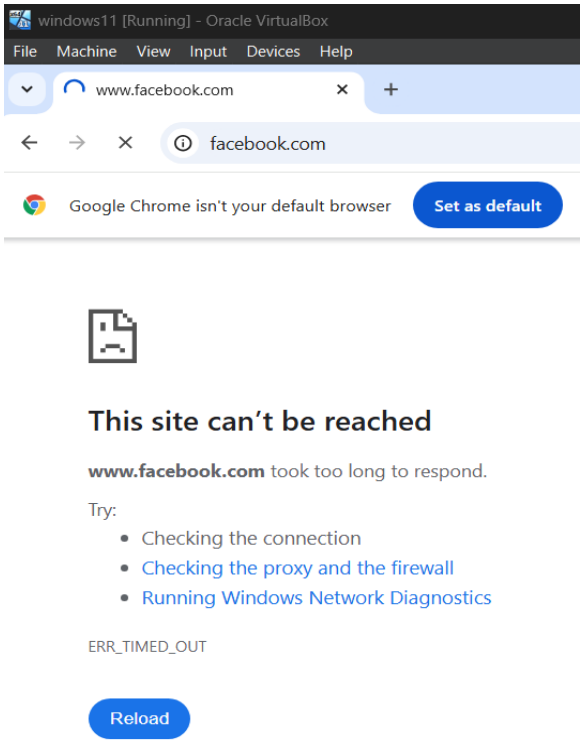
bertujuan untuk memastikan bahwa semua aturan yang telah dikonfigurasi bekerja sebagaimana mestinya dalam membatasi akses pengguna ke situs yang tidak diizinkan. Tampilan situs web sesudah dibatasi menggunakan *layer7 protocol*, pada gambar berikut.



Gambar 9. Tampilan Situs Instagram Tidak Dapat di akses



Gambar 10. Tampilan Situs Tiktok Tidak Dapat di akses



Gambar 11. Tampilan Situs Facebook Tidak Dapat di akses

Pengujian yang dilakukan meliputi pengalamatan IP pada user kemudian mengkonfigurasi *firewall* berbasis mikrotik dengan metode Layer7 *Protocol.* Ketika seluruh konfigurasi selesai maka melakukan pengujian dengan membuka situs-situs website yang telah diterapkan pembatasan untuk diakses oleh siswa ataupun user di lingkungan sekolah. Hasilnya menunjukan bahwa pengujian penerapan *firewall* untuk membatasi akses internet pada beberapa situs website yang tidak mendukung pembelajaran semua pengujian dinyatakan sukses yang dapat dilihat pada gambar 9, gambar 10, gambar 11 dan juga tabel 1.

4.4. Situs yang di Blokir

Pengumpulan data terkait situs-situs yang diblokir di SMK Al - Hikam dilandasi oleh kebijakan institusi yang bertujuan untuk menciptakan suasana dan lingkungan pembelajaran yang lebih kondusif, terfokus, serta bebas dari gangguan yang tidak relevan dengan kegiatan akademik. Kebijakan ini diterapkan guna membatasi akses terhadap situs-situs yang dinilai tidak mendukung proses belajar mengajar atau bahkan berpotensi mengganggu konsentrasi siswa selama berada di lingkungan sekolah.

Adapun kategori situs yang menjadi objek pemblokiran meliputi berbagai jenis, seperti situs media sosial, Situs media sosial seperti Tiktok, Instagram, dan Facebook dipilih untuk diblokir karena telah terbukti dapat menyita perhatian pengguna, termasuk siswa, dari aktivitas inti mereka yaitu belajar dan mengerjakan tugas. Tidak hanya itu, keberadaan situs-situs tersebut juga menyebabkan peningkatan penggunaan *bandwidth* secara drastis, yang pada

akhirnya dapat mengganggu stabilitas jaringan dan menurunkan kualitas akses internet bagi siswa yang sedang menggunakan jaringan untuk keperluan akademik atau akses ke platform pembelajaran daring.

Dalam proses pengumpulan data, digunakan acuan berupa daftar situs blacklist yang bersumber dari penyedia layanan atau sumber eksternal terpercaya. Daftar ini telah disusun berdasarkan klasifikasi jenis konten serta tingkat risiko yang ditimbulkan oleh masing-masing situs. Pendekatan semacam ini memungkinkan penerapan sistem pemblokiran menjadi lebih sistematis dan selektif, sehingga hanya situs-situs yang benar-benar mengganggu proses pembelajaran yang dibatasi. Penerapan pembatasan hak akses ini kemudian dilakukan dengan memanfaatkan teknologi *Layer7 Protocol* berbasis MikroTik, yang memungkinkan administrator jaringan untuk secara fleksibel dan efisien mengatur, mengawasi, serta memfilter lalu lintas data internet di sekolah. Dengan cara ini, lingkungan sekolah dapat difungsikan secara maksimal untuk mendukung kegiatan akademik dan menunjang prestasi belajar siswa.

Tabel 1. Daftar situs kategori Media Sosial yang di Blokir

No	Alamat website	status	Hasil pengujian
1.	Instagram.com	Drop	Sukses
2.	Tiktok.com	Drop	Sukses
3.	Facebook.com	Drop	Sukses

Tabel 1 menunjukkan daftar situs yang termasuk dalam kategori media sosial dan telah diblokir. Situs-situs tersebut antara lain Facebook.com, Instagram.com, dan Tiktok.com. Status untuk semua situs ini adalah *Drop*, yang berarti aksesnya dibatasi atau ditolak. Berdasarkan hasil pengujian, seluruh proses pemblokiran terhadap situs-situs ini dinyatakan berhasil atau "Sukses". Untuk situs website youtube tidak diblokir karena bisa diakses untuk mendukung pembelajaran.

5. KESIMPULAN DAN SARAN

Dari hasil penelitian ini, dapat disimpulkan bahwa penerapan *Layer7 Protocol* pada Mikrotik untuk membatasi akses internet yang digunakan siswa dinyatakan sukses dengan beberapa pengujian membuka situs-situs yang diterapkan konfigurasi *Laayer7 Protocol*. Pada gambar 9 menunjukkan bahwa situs Instagram tidak dapat diakses, gambar 10 enunjukkan bahwa situs tiktok idak dapat diakses, gambar 11 menunjukkan bahwa situs facebook tidak dapat diakses. Dari hasil tersebut maka penerapan *Firewall* dan *Filtering Firewall* berbasis miktorik dengan metode *Layer7 Protocol* sukses diterapkan.

Dari hasil yang diperoleh masih ada beberapa kekurangan dari segi situs-situs website yang masih sedikit untuk pembatasan aksesnya yang hanya terdiri dari situs sosmed instagram, tiktok, facebook. Saran untuk penelitian selanjutnya yaitu menambahkan situs-situs website yang tidak mendukung seperti situs sosmed, perjudian, dan lain sebagainya. Kemudian dari segi metode mungkin bisa menambahkan metode firewall lainnya seperti web proxy untuk memaksimalkan penerapan *firewall* dan *filtering firewall.*

DAFTAR PUSTAKA

[1] A. Ramadhani, N. Palasara, and A. Gani, "Filtering Firewall dan Manajemen Bandwidth untuk Keamanan Jaringan pada Kelurahan Buaran Indah," *remik*, vol. 9, no. 1, pp. 346–355, Jan. 2025, doi: 10.33395/remik.v9i1.14482.

[2] M. R. Perdana *et al.*, "2 ND MDP STUDENT CONFERENCE (MSC) 2023 52| Universitas Multi Data Palembang FIREWALL DAN WEB FILTERING DENGAN MIKROTIK PADA DISKOMINFO KOTA PALEMBANG".

[3] Sutiman and A. Gunawan, "FIREWALL PORT SECURITY SWITCH UNTUK KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN CISCO ROUTER 1600S PADA PT. TIRTA KENCANA TATA WARNA SUKABUMI," *CONTEN : Computer and Network Technology*, vol. 1, no. 1, pp. 13–22, 2021, [Online]. Available: http://jurnal.bsi.ac.id/index.php/conten

[4] B. Cahya, F. Rizki, A. Sutiyo, Y. El Saputra, and M. Elfarizi, "IMPLEMENTASI FIREWALL PADA MIKROTIK UNTUK KEAMANAN JARINGAN," 2023. [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[5] C. Kamila Wilujeng, A. Voutama Sistem Informasi, U. Singaperbangsa Karawang Jl HSRonggo Waluyo, T. Timur, and J. Barat, "IMPLEMENTASI FIREWALL FILTER RULES SEBAGAI FILTERING CONTENT PADA JARINGAN KOMPUTER MENGGUNAKAN MIKROTIK," 2024.

[6] E. Eben, M. Mukramin, and H. Abduh, "PENGEMBANGAN MANAJEMEN KEAMANAN JARINGAN NIRKABEL (WIFI) MENGGUNAKAN ROUTERBOARD MIKROTIK DAN FIREWALL PADA SMK KRISTEN PALOPO," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 3, Aug. 2024, doi: 10.23960/jitet.v12i3.4716.

[7] C. Kamila Wilujeng, A. Voutama Sistem Informasi, U. Singaperbangsa Karawang Jl HSRonggo Waluyo, T. Timur, and J. Barat, "IMPLEMENTASI FIREWALL FILTER RULES SEBAGAI FILTERING CONTENT PADA JARINGAN KOMPUTER MENGGUNAKAN MIKROTIK," 2024.

[8] K. Aziz, S. Zakir, W. Aprison, and L. Efriyanti, "IMPLEMENTASI KEAMANAN JARINGAN DENGAN METODE FIREWALL FILTERING MENGGUNAKAN MIKROTIK DI SMKN 3 PAYAKUMBUH," 2024.

[9] A. Irfan, A. Z. Nusri, Z. Rachmat, and S. Wulandari, "Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System (WIDS)," *Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI)*, vol. 7, no. 1, pp. 110–119, Apr. 2024, doi: 10.57093/jisti.v7i1.195.

[10] B. Cahya, F. Rizki, A. Sutiyo, Y. El Saputra, and M. Elfarizi, "IMPLEMENTASI FIREWALL PADA MIKROTIK UNTUK KEAMANAN JARINGAN," 2023. [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[11] 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," 2023.