SKANIKA: Sistem Komputer dan Teknik Informatika
Volume 8, Nomor 1, Januari 2025, Halaman 46-59 E-ISSN: 2721-4788

Implementasi Web *Filtering Firewall* untuk Keamanan pada Jaringan Internet di Pondok Pesantren Al Hidayah Kebumen

Ahmad Sukron Ma'mun[1*], Ghufron Zaida Muflih[2]
[1,2]Fakultas Teknik, Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama, Kebumen, Indonesia
E-mail : [1*]ahmdsukronm@gmail.com, [2]ghufron.zaida@umnu.ac.id
(* : corresponding author)

Abstrak

Di era digital saat ini, akses internet yang bebas dapat memberikan dampak positif maupun negatif, khususnya di lingkungan pendidikan seperti pondok pesantren. Penelitian ini bertujuan untuk mengimplementasikan sistem web *filtering firewall* berbasis *Mikrotik RouterOS* guna meningkatkan keamanan jaringan internet di Pondok Pesantren Al Hidayah Kebumen menggunakan *mikrotik* RB951Ui-2HnD sebagai perangkat pendukung untuk mengelola akses jaringan dan aplikasi *winbox* untuk konfigurasi ke *router mikrotik*. Penelitian ini mengadopsi pendekatan *web proxy* yang bertujuan untuk membatasi akses ke konten negatif seperti pornografi, judi *online*, dan *game online* yang dapat mengganggu proses belajar para santri. Metode pengembangan yang diterapkan adalah model *waterfall*, yang meliputi tahapan analisis, desain, implementasi, pengujian, dan pemeliharaan. Hasil implementasi menunjukkan bahwa sistem mampu memblokir situs-situs yang tidak diinginkan secara efektif, sehingga menciptakan lingkungan internet yang lebih aman dan kondusif untuk kegiatan belajar. Penelitian ini dapat memberikan solusi yang efektif dalam pengelolaan dan pengendalian akses internet di Pondok Pesantren Al Hidayah Kebumen.

Kata kunci: Web *Filtering Firewall*, Keamanan Jaringan, *Mikrotik RouterOS*, Pondok Pesantren

Abstract

In the digital era, unrestricted internet access can have both positive and negative impacts, particularly in educational settings such as Islamic boarding schools (pondok pesantren). This study aims to implement a web filtering firewall system based on Mikrotik RouterOS to enhance internet network security at Al Hidayah Islamic Boarding School in Kebumen. Utilizing the Mikrotik RB951Ui-2HnD device to manage network access and winbox for router configuration, this research applies a web proxy approach to restrict access to negative content such as pornography, online gambling, and online games, which may interfere with students' learning processes. The development process follows the Waterfall model, encompassing the stages of analysis, design, implementation, testing, and maintenance. Results from the implementation indicate that the system effectively blocks unwanted websites, thereby fostering a safer and more conducive internet environment for educational activities. This research can provide an effective solution in managing and controlling internet access at the Al Hidayah Islamic Boarding School, Kebumen.

Keywords: *Web Filtering Firewall, Network Security, Mikrotik RouterOS, Islamic Boarding School*

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer di era digital saat ini berlangsung dengan sangat pesat. Hal ini terlihat dari perkembangan pada bidang perangkat keras ataupun perangkat lunak. Jaringan komputer sudah seperti kebutuhan pokok bagi manusia, karena segala informasi dapat diakses secara mudah dengan internet menggunakan perangkat seperti komputer, laptop, tablet, atau *smartphone*[1]. *Wi-Fi* merupakan bentuk perkembangan teknologi yang memungkinkan koneksi tanpa harus menggunakan kabel atau disebut dengan jaringan nirkabel [2]. Jaringan nirkabel merupakan jenis jaringan komputer yang memanfaatkan gelombang elektromagnetik sebagai media untuk mengirimkan data, dan dikenal dengan jaringan *WLAN* [3]. Saat ini penggunaan *Wi-Fi* sudah sangat umum ditemukan, bahkan hampir di semua tempat seperti kafe, sekolah, kampus, rumah dan kantor, termasuk di Pondok Pesantren Al Hidayah Kebumen [4].

Pondok Pesantren Al Hidayah adalah lembaga pendidikan yang tepatnya berada di dukuh Wonoyoso, kelurahan Bumirejo, kecamatan Kebumen, Kabupaten Kebumen. Layaknya lembaga pendidikan lainnya, Pondok Pesantren Al Hidayah juga menyediakan jaringan internet untuk

mendukung berbagai aktivitas kepesantrenan serta proses belajar mengajar bagi para santri. Pesantren Al Hidayah mempunyai perangkat jaringan yang terhubung ke seluruh komplek diantaranya ruang kantor, komplek putra, komplek putri, dan rumah pengasuh yang digunakan oleh para santri untuk kegiatan belajar mengajar, serta para guru dan pengasuh pesantren melalui jaringan hotspot [5]. Internet memungkinkan akses bebas ke berbagai informasi, meskipun tidak semua konten bermanfaat. Beberapa konten yang tidak pantas diantaranya seperti pornografi, judi *online*, *game online* dan konten-konten lainnya dapat menimbulkan dampak buruk untuk para santri [6]. Pemakaian internet juga dapat menyebabkan efek candu pada anak-anak dan remaja, yang dapat menyebabkan perubahan pola pikir dan ketidakstabilan emosional, tetapi tidak selalu mengarah pada perilaku kenakalan remaja yang membutuhkan perawatan khusus [7].

Melihat permasalahan tersebut, perlu adanya pembatasan pada sistem jaringan internet di Pondok Pesantren Al Hidayah untuk menciptakan lingkungan internet yang sehat dan positif. Salah satu caranya adalah dengan menerapkan web *fitering firewall* melalui *Mikrotik RouterOS* pada jaringan internet yang ada di pondok pesantren. *Mikrotik RouterOS* merupakan suatu sistem operasi jaringan yang sangat umum dan banyak digunakan, karena menyediakan fitur *firewall* yang sangat lengkap yang mencakup berbagai kemampuan, seperti filter konten**,** filter IP, filter paket**,** serta beragam fitur tambahan lainnya [8]. *Mikrotik* digunakan sebagai perangkat pendukung untuk mengelola akses jaringan, dan proses konfigurasinya dapat dilakukan melalui aplikasi *winbox*. Aplikasi ini disediakan *mikrotik* untuk dapat mempermudah proses konfigurasi pada perangkat jaringan [9]. *Firewall* pada layanan *router mikrotik* mampu mengatasi permasalahan ini, karena *firewall* berfungsi melindungi jaringan baik dari sisi dalam maupun luar melalui pengaturan port yang tersedia [10]. Dengan adanya layanan *mikrotik*, *firewall* dapat juga digunakan sebagai pembatas pada port-port yang diizinkan untuk akses keluar dan masuk pada jaringan [11].

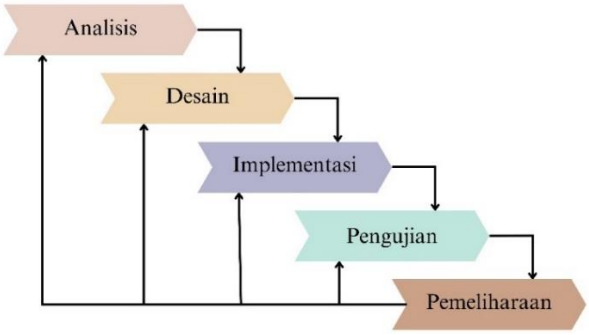
Penelitian *filtering* menggunakan mikrotik, sebelumnya menerapkan *router* Mikrotik dengan metode *Layer 7* untuk memblokir akses ke situs seperti *YouTube, Facebook, dan Instagram* di sistem jaringan *Garage Freshmart*, karena penggunaan internet dan media sosial yang tidak terkendali oleh karyawan selama jam kerja. Hasil penelitian menunjukkan bahwa penerapan *router mikrotik* mampu memblokir situs tersebut pada sistem jaringan *Garage Freshmart* [12]. Selanjutnya, implementasi *web proxy* menggunakan *Mikrotik RouterOS* untuk meningkatkan kinerja jaringan internet. Metode *filtering* dan *caching* pada *Mikrotik RouterOS* mampu meningkatkan keamanan jaringan serta kinerja internet di lingkungan kantor [13]. Penelitian berikutnya melakukan kontrol akses internet siswa di sekolah untuk mencegah akses ke konten berbahaya atau tidak sesuai selama pembelajaran. Pemblokiran dapat dilakukan secara efektif melalui *packet filtering* menggunakan perangkat *mikrotik,* sehingga siswa tidak dapat mengakses situs yang tidak diizinkan saat menggunakan jaringan sekolah [14]. Penelitian [15] menerapkan *filter rule* dan *Layer 7 Protocol* pada router Mikrotik untuk membatasi akses ke game *online* dan media sosial selama jam kerja. Hasil penelitiannya menunjukkan bahwa akses tersebut berhasil diblokir selama jam kerja.

Penelitian ini berbeda dari penelitian terdahulu dengan menghadirkan inovasi berupa pembaruan *regex* secara otomatis berdasarkan jadwal yang telah ditentukan. Pendekatan ini mengatasi keterbatasan metode sebelumnya, yang umumnya mengandalkan pembaruan manual atau berbasis kejadian tertentu, sehingga meningkatkan efisiensi dan keandalan sistem dalam menghadapi perubahan data atau pola yang dinamis. Penelitian ini bertujuan untuk menerapkan sistem web filtering *firewall* pada jaringan internet di Pondok Pesantren Al Hidayah Kebumen. Sistem dirancang untuk membatasi akses ke berbagai konten negatif, termasuk situs-situs yang mengandung unsur pornografi, perjudian, *game online* dan situs lainnya yang dapat berdampak buruk pada pengguna layanan internet di lingkungan pondok pesantren, khususnya bagi para santri. Memanfaatkan web *filtering firewall* melalui perangkat *Mikrotik RouterOS,* untuk menciptakan jaringan internet yang aman dan juga mendukung aktivitas belajar mengajar yang terawasi di lingkungan pesantren. Diharapkan, sistem yang diterapkan mampu secara efektif mengurangi risiko paparan konten yang berbahaya, amoral, sekaligus mendorong terciptanya

suasana belajar yang lebih kondusif, selaras dengan nilai-nilai keagamaan, moral dan pendidikan yang dianut pesantren.

2. METODE PENELITIAN

Metode meliputi serangkaian langkah yang dilakukan, mulai dari melakukan survei, mengidentifikasi dan menggambarkan permasalahan yang ada, merumuskan masalah yang ditemukan, hingga menganalisis secara mendalam untuk menentukan sifat dan karakteristik dari masalah [16]. Metode *waterfall* digunakan sebagai model pengembangan supaya tujuan lebih jelas dan mengurangi perubahan signifikan di setiap tahap. Metode *waterfall* memastikan bahwa setiap langkah kerja dilakukan secara berurutan, di mana setiap tahapnya harus sudah selesai sebelum melangkah ke tahap selanjutnya. Tahapan dalam proses implementasi web *filtering firewall* meliputi analisis**,** desain**,** implementasi**,** pengujian**,** dan pemeliharaan [17]. Metode *waterfall* seperti pada Gambar 1.



Gambar 1. Metode *Waterfall*

2.1 Analisis

Dilakukan pengumpulan berbagai informasi yang diperlukan untuk penelitian terkait penerapan web *filtering firewall* pada jaringan internet. Proses analisis ini penting untuk mengidentifikasi permasalahan yang muncul dalam upaya menciptakan internet sehat di Pondok Pesantren Al Hidayah Kebumen. Langkah-langkah yang diambil antara lain mencakup identifikasi masalah melalui studi literatur, observasi langsung, dan wawancara dengan administrator jaringan untuk memperoleh hasil mengenai dampak yang mungkin timbul apabila akses internet dibiarkan tanpa batas, yang memungkinkan akses mudah ke situs-situs berbahaya dan merugikan.

2.2 Desain

Tahap desain, merupakan proses perancangan sistem yang hendak diterapkan untuk menangani masalah yang telah diidentifikasi pada tahap analisis sebelumnya. Desain ini mencakup pengaturan *filter* konten yang disesuaikan dengan kebutuhan pesantren, sehingga proses pembatasan akses tetap efektif namun tidak mengganggu akses ke situs-situs edukatif atau informasi positif lainnya.

2.3 Implementasi

Tahap implementasi, yakni menjalankan rancangan yang telah disusun 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 sesuai, seperti situs pornografi, judi *online*, dan *game online.*

2.4 Pengujian

Tahap ini bertujuan untuk menguji *mikrotik* yang telah dikonfigurasi untuk memastikan sistem berfungsi dengan baik dan sesuai dengan standar kebutuhan.

2.5 Pemeliharaan

Tahap terakhir adalah pemeliharaan yang menjadi kunci untuk memastikan sistem tersebut tetap berfungsi optimal dalam menjaga keamanan dan produktivitas akses internet di lingkungan pesantren.

3. HASIL DAN PEMBAHASAN

3.1 Analisis

a. Analisis Permasalahan

Peneliti melakukan observasi dan wawancara di Pondok Pesantren Al Hidayah Kebumen pada tanggal 4 Oktober 2024 yang berfokus pada penggunaan jaringan internet di lingkungan pondok pesantren. Diperoleh data bahwa belum adanya penerapan *filtering* pada jaringan internet yang ada, sehingga penggunaan jaringan internet masih bebas untuk mengakses sembarang situs. Peneliti melakukan pengujian awal secara acak terhadap situs pornografi, judi *online* dan *game online* menggunakan jaringan internet di Pondok Pesantren Al Hidayah Kebumen sebelum diterapkan web *filtering firewall* dan didapatkan bahwa situs tersebut masih sangat mudah diakses. Akses internet tanpa batasan dapat mempermudah santri mengakses konten yang tidak sesuai, sehingga berpotensi mengganggu konsentrasi belajar dan menghambat pencapaian tujuan pendidikan di pesantren.

b. Analisis Tindak Lanjut

Dari permasalahan yang ada, penulis mengusulkan penerapan web *filtering firewall* pada jaringan internet di Pondok Pesantren Al Hidayah Kebumen dengan menambahkan perangkat *router mikrotik* sebagai perangkat pendukung untuk mengelola akses jaringan. Penerapan ini bertujuan untuk membatasi akses pada jaringan internet yang ada di pondok pesantren, guna melindungi para penggunanya dari konten yang tidak diinginkan. Pembatasan akses internet mencakup situs pornografi, judi *online,* dan *game online.*

c. Analisis Kebutuhan Sistem

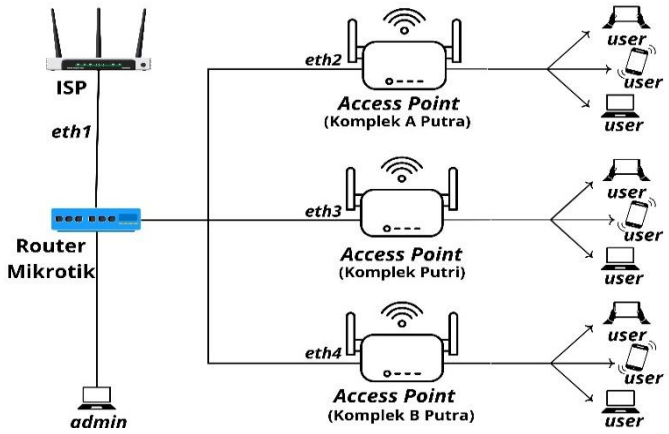
Dalam proses ini, penulis melakukan analisis terhadap kebutuhan sistem yang diperlukan untuk penelitian, mencakup kebutuhan perangkat keras dan perangkat lunak yang mendukung. Analisis kebutuhan sistem seperti pada Tabel 1 berikut.

Tabel 1. Analisis Kebutuhan

No	Perangkat/*Tool*	Spesifikasi/Keterangan
1	Laptop	*HP Intel(R) Celeron(R) N4120 CPU @ 1.10GHz 1.10 GHz*
2	*Router Mikrotik*	RB951Ui-2HnD
3	*Windows 11 x64*	Sistem operasi
4	*Winbox*	Aplikasi untuk konfigurasi ke *Router Mikroik*
5	*Google Chrome*	Aplikasi yang digunakan untuk pengujian

3.2 Desain

Desain penerapan web *filtering firewall* dirancang dengan mengonfigurasi *router mikrotik* untuk memfilter dan memblokir akses ke situs-situs negatif seperti pornografi, judi *online*, dan *game online* yang dapat mengganggu konsentrasi serta kesehatan mental para santri. Penulis telah merancang topologi jaringan yang akan digunakan untuk mengimplementasikan web *filtering firewall* sebagaimana ditunjukkan pada Gambar 2.



Gambar 2. Topologi Jaringan Setelah Penerapan Web *Filtering Firewall*

Topologi pada Gambar 2 menggambarkan proses penelitian yang bertujuan untuk mengatur sistem web *filtering* pada jaringan internet di Pondok Pesantren Al Hidayah Kebumen. *Mikrotik* berperan sebagai server yang terhubung langsung dengan ISP *(Internet Service Provider),* kemudian mendistribusikan koneksi internet melalui *access point* kepada perangkat pengguna seperti *handphone*, laptop, dan komputer. Sebelum koneksi internet mencapai *access point*, dilakukan konfigurasi pada *mikrotik* menggunakan *Layer 7 Protocol dan Regex*, yang berfungsi menyaring konten-konten tertentu dan memanfaatkan aplikasi *winbox* sebagai alat dalam pengelolaannya.

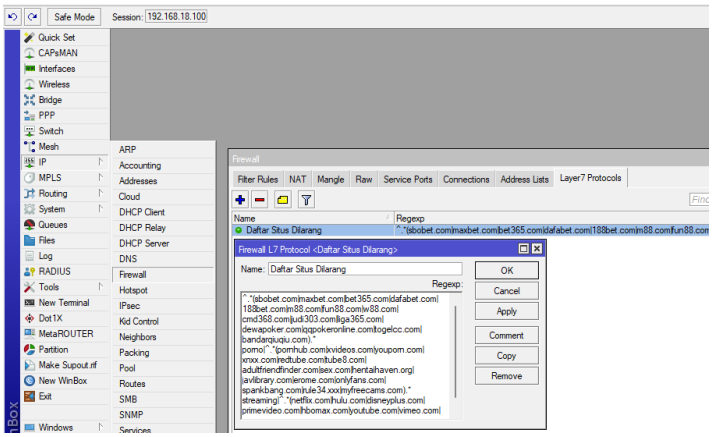
3.3 Implementasi

a. Proses Pemblokiran Situs – Situs Pornografi dan Judi *Online*

Pemblokiran situs pornografi dan judi *online* dilakukan dengan mengkonfigurasi mikrotik menggunakan *Layer 7 Protocol dan regex*. Langkah-langkah dalam melakukan pemblokiran adalah sebagai berikut.

1) Konfigurasi *Layer 7 Protocols*

Masuk ke menu IP lalu *firewall* dan pilih tab *Layer 7 protocols*, masukkan situs atau alamat web yang ingin di-*block* dengan *script layer 7 ^.+(Domain|Domain).*$* seperti pada Gambar 3.



Gambar 3. Konfigurasi Layer 7 *Protocols*

Daftar *Regex* yang digunakan untuk pemblokiran seperti pada Tabel 2.

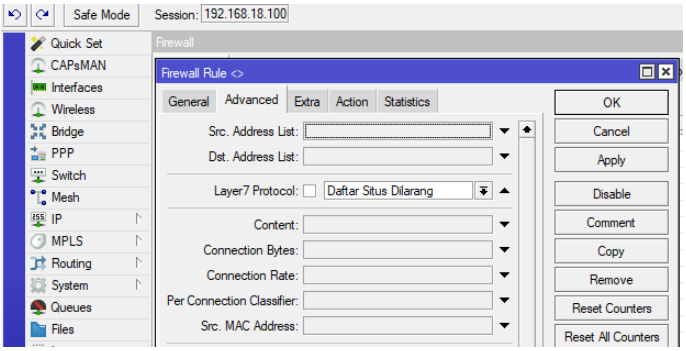
Tabel 2. Daftar *Regex*

Nama Situs	Filter *Regex*
Situs Pornografi	*|^.*(pornhub\.com|xvideos\.com|youporn\.com|xnxx\.com|redtube\.com |tube8\.com|adultfriendfinder\.com|sex\.com|hentaihaven\.org |javlibrary\.com|erome\.com|onlyfans\.com|spankbang\.com|rule34\.xxx |myfreecams\.com).*$*
Situs Judi *Online*	*|^.*(sbobet\.com|maxbet\.com|bet365\.com|dafabet\.com|188bet\.com |m88\.com|fun88\.com|w88\.com|cmd368\.com|judi303\.com |liga365\.com|dewapoker\.com|qqpokeronline\.com|togelcc\.com |bandarqiuqiu\.com).*$*

2) Menambahkan Aturan *Firewall* untuk Memblokir Situs

Menambahkan aturan firewall untuk memblokir situs dengan membuka menu IP, dan memilih submenu *Firewall.* Pada tab *Filter Rules,* memilih *Chain Forward* di tab General untuk memblokir data yang melewati *mikrotik.* Memilih protokol 6 (TCP) untuk membatasi lalu lintas berbasis TCP, karena protokol ini umum digunakan oleh platform berbasis web seperti situs pornografi dan judi *online*. Menerapkan aturan pada semua antarmuka *ethernet* dengan memilih opsi *All Ethernet* di menu *In. Interface*.

Pada tab advance isi kolom *layer 7 protocol* dengan blok situs yang sudah dibuat sebelumnya, dan pada tab *action* pilih drop untuk memblokir akses ke situs. Tampilan tab *advance* seperti pada Gambar 4.



Gambar 4. Filter Rules Tab Advanced

3) Mengonfigurasi Pembaruan Otomatis File *Regex*

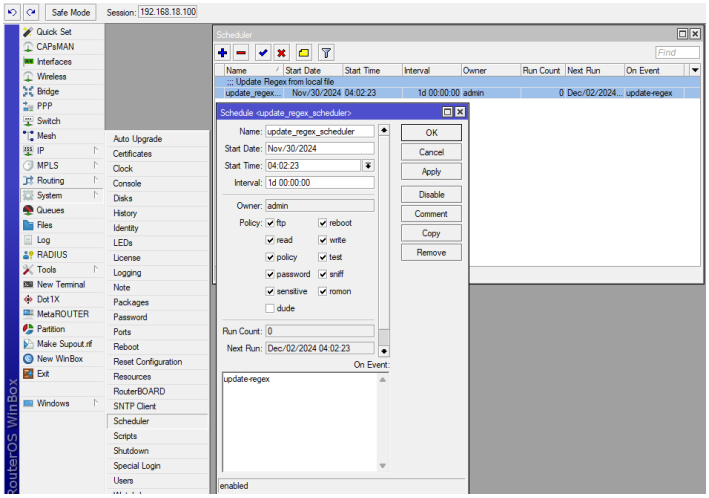
Buka aplikasi winbox pada mikrotik dan navigasikan ke menu *System, Scripts* untuk mengelola skrip otomatis. Selanjutnya, membuat skrip baru, lalu beri nama *"update-regex"*, agar mudah dikenali dan diidentifikasi dalam daftar skrip yang tersedia. Daftar skrip yang digunakan seperti pada Tabel 3.

Tabel 3. Daftar Skrip

Skrip	Keterangan

:local fileContents [/file get regex_list.txt contents]
:foreach line in=[:toarray $fileContents] do={
:if ([:find $line "#"] != 0) do={
:local separatorPos [:find $line "|"]
:local category [:pick $line 0 $separatorPos]
:local pattern [:pick $line ($separatorPos + 1) [:len $line]]
:log info ("Kategori: " . $category . " | Regex: " . $pattern)
:if ($category = "judi") do={
/ip firewall layer7-protocol set [find name="Daftar Situs Dilarang"] regexp=$pattern }
:if ($category = "porno") do={
/ip firewall layer7-protocol set [find name="Daftar Situs Pornografi"] regexp=$pattern }
}
}
	Tujuan dari script ini adalah untuk mempermudah administrator jaringan dalam mengelola dan memperbarui aturan *firewall mikrotik* secara otomatis berdasarkan kategori situs yang ingin diblokir. Dengan membaca daftar kategori dan pola regex dari file eksternal *(regex_list.txt)*, script ini mampu memproses setiap entri untuk kemudian mengimplementasikan aturan blokir menggunakan fitur *Layer7 Protocol*. Hal ini bertujuan untuk meningkatkan efisiensi dalam pengelolaan jaringan dengan membatasi akses ke situs tertentu, seperti situs perjudian atau pornografi, sehingga mendukung keamanan dan produktivitas penggunaan jaringan.

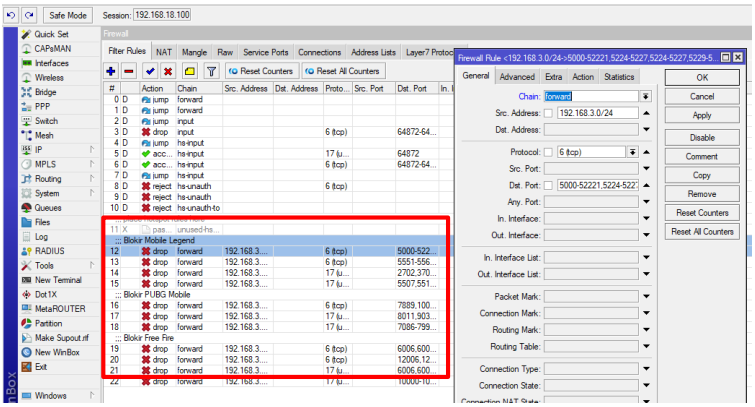
Untuk membuat jadwal otomatis pembaruan file *Regex* pada *mikrotik*, buka menu *System, Scheduler* untuk menambahkan tugas baru. Beri nama, *"update_regex_scheduler"*, kemudian atur jadwal *Start Time* pukul 00:00 dan *Interval* "1d 00:00:00" untuk pembaruan harian. Klik OK untuk menyimpan, dan sistem akan menjalankan pembaruan file *regex* secara otomatis sesuai jadwal. Langkah membuat jadwal pembaruan *regex* otomatis seperti pada Gambar 5.



Gambar 5. Membuat Jadwal Pembaruan *Regex* Otomatis

b. Proses Pemblokiran *Game Online*

Pemblokiran *game online* digunakan port TCP dan UDP dari *game* tersebut. Pada penelitian ini pemblokiran dilakukan terhadap 3 jenis *game online* yaitu *Mobile Legend*, *PUBG Mobile*, dan *Free Fire*. Tampilan tahap pemblokiran *game online* seperti Gambar 6 berikut.



Gambar 6. Tahap Pemblokiran Game *Online*

Proses pemblokiran dengan mengakses *winbox*, selanjutnya mengakses *firewall*. Tampilan *firewall* muncul seperti pada Gambar 6. Untuk memulai proses pemblokiran menggunakan port-port yang digunakan oleh *game online*, menggunakan *Firewall Rule* untuk melakukan konfigurasi pemblokiran. Pada kolom *Chain* pilih *Forward*, pada bagian *Protocol*, memilih TCP. Kolom *Dst. Port*, mengisi port yang digunakan oleh *game online* yang berbasis TCP. Proses ini juga dapat dilakukan untuk port UDP jika diperlukan.

Setelah menyelesaikan pengaturan pada *firewall rule*, TCP dan UDP, langkah berikutnya adalah membuka tab *action* dan memilih *action drop*. Daftar port UDP dan TCP yang digunakan untuk pemblokiran seperti pada Tabel 4.

Tabel 4. Daftar Port TCP dan UDP

Nama *Game*	Port Yang Digunakan
Mobile Legends	**TCP**: 5000-52221, 5224-5227, 5224-5227, 5229-5241, 5243-5287, 5289 5352,5354-5509,5517,5520-5529 || **TCP**: 5551-5569, 5601-5700, 8443, 9000-9010, 9443, 10003, 30000-30900 || **UDP**: 2702, 3702, 4001-4009, 5000-5221, 5224-5241, 5243-5289, 5289-5352, 5354-5509 || **UDP**: 5507, 5517-5529, 5551-5569, 5601-5700, 8001, 8130
PUBG Mobile	**TCP**: 6006, 6008, 6674, 7000-7999, 8001-8012, 9006, 9137, 10000-10015, 11000 11019 || **TCP**: 12006, 12008, 13006, 15006, 20561, 39003, 39006, 39698, 39779, 39800 || **UDP**: 6006, 6008, 6674, 7000-7999, 8008, 8001-8012, 8130, 8443, 9008, 9120 || **UDP**: 7086-7995, 10039, 10096, 11096, 11455, 12070-12460, 13894,13972, 41182-41192
Free Fire	**TCP**: 6006, 6008, 6674, 7000-7999, 8001-8012, 9006, 9137, 10000-10015, 11000-11019 || **UDP**: 8008, 8001-8012, 8130, 8443, 9008, 9120, 10000-10015, 10100, 11000-11019, 12008, 13008 || **UDP**: 7086-7995, 10039, 10096, 11096, 11455, 12070-12460, 13894, 13972, 41182-41192

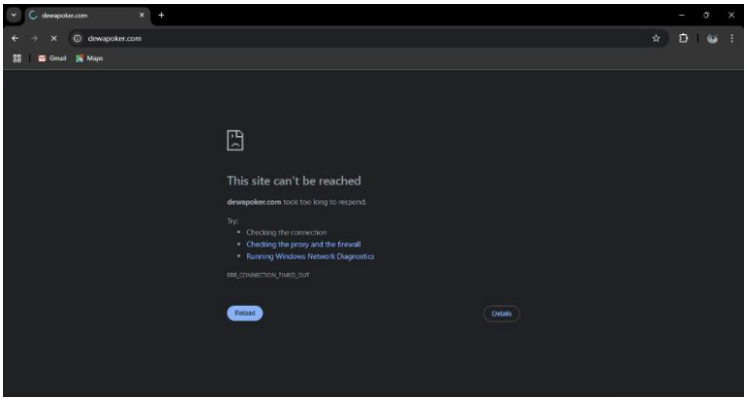
3.4 Pengujian

Pengujian sistem *web filtering* untuk situs pornografi dan judi *online* melalui *Google Chrome* untuk memastikan efektivitas pemblokiran. Konfigurasi yang berhasil menunjukkan situs target tidak dapat diakses setelah konfigurasi diterapkan. Pengujian ini mencakup akses sebelum dan sesudah penerapan sistem *filtering* untuk memastikan fungsinya berjalan optimal.

a. Pengujian Situs Blokir

Pada tahap ini, uji akses dilakukan terhadap salah satu situs judi *online*. Hasil menunjukkan bahwa sebelum penerapan sistem *filtering* pengguna jaringan dapat mengakses situs tersebut tanpa adanya hambatan.

Selanjutnya, dilakukan uji akses setelah diterapkannya sistem web *filtering* pada jaringan internet. Akses ke domain *dewapoker.com* diblokir, sehingga halaman web tersebut tidak akan dapat ditampilkan atau diakses. Pemblokiran ini memastikan bahwa pengguna jaringan tidak dapat mengunjungi situs tersebut. Hasil pengujian seperti pada Gambar 7.

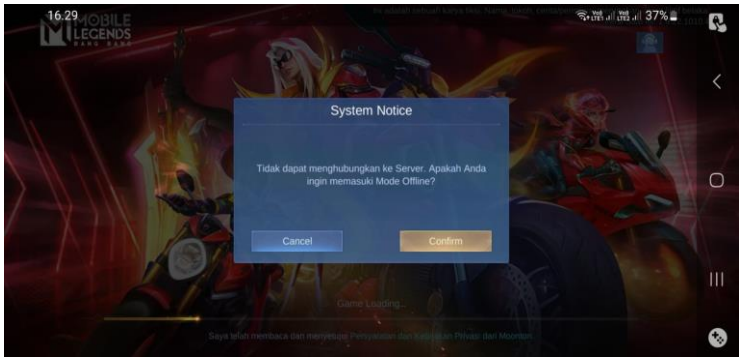


Gambar 7. Tampilan Situs Sesudah di Blokir

b. Pengujian *Game Online*

Pengujian terhadap pemblokiran *game online* dilakukan dengan mencoba mengakses *Game Mobile Legends* menggunakan perangkat yang terhubung dengan jaringan internet di Pondok Pesantren Al Hidayah Kebumen. Hasil pengujian menunjukan bahwa sebelum dilakukan pemblokiran, *game Mobile Legends* masih dapat diakses menggunakan jaringan internet.

Berikutnya, akan dilakukan uji akses setelah diterapkannya sistem *filtering* pada jaringan internet sebagaimana ditunjukkan Gambar 8.



Gambar 8. Tampilan *Game Online* Sesudah di Blokir

Karena akses diblokir, *game Mobile Legends* hanya akan menampilkan proses *loading* yang berkelanjutan dan tidak memungkinkan pengguna untuk masuk ke dalam *game* tersebut.

Hasil pengujian terhadap akses situs setelah diterapkan sistem *filtering* yang menjadi target pemblokiran mencakup 3 jenis konten seperti pada Tabel 5.

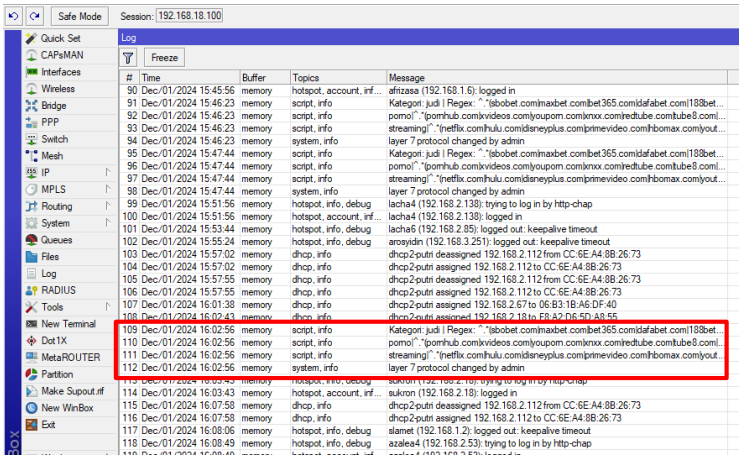
Tabel 5. Hasil Pengujian

Jenis Konten	Konten	Keterangan
Pornografi	*pornhub\.com*	Berhasil Terblokir
	xvideos\.com	Berhasil Terblokir
	youporn\.com	Berhasil Terblokir
	xnxx\.com	Berhasil Terblokir
	redtube\.com	Berhasil Terblokir
	tube8\.com	Berhasil Terblokir
	adultfriendfinder\.com	Berhasil Terblokir
	sex\.com	Berhasil Terblokir
	hentaihaven\.org	Berhasil Terblokir
	javlibrary\.com	Berhasil Terblokir
	erome\.com	Berhasil Terblokir
	onlyfans\.com	Berhasil Terblokir
	spankbang\.com	Berhasil Terblokir
	rule34\.xxx	Berhasil Terblokir
	myfreecams\.com	Berhasil Terblokir
Judi *Online*	*sbobet\.com*	Berhasil Terblokir
	maxbet\.com	Berhasil Terblokir
	bet365\.com	Berhasil Terblokir
	dafabet\.com	Berhasil Terblokir
	188bet\.com	Berhasil Terblokir
	m88\.com	Berhasil Terblokir
	fun88\.com	Berhasil Terblokir
	w88\.com	Berhasil Terblokir
	cmd368\.com	Berhasil Terblokir
	judi303\.com	Berhasil Terblokir
	liga365\.com	Berhasil Terblokir
	dewapoker\.com	Berhasil Terblokir
	qqpokeronline\.com	Berhasil Terblokir
	togelcc\.com	Berhasil Terblokir
	bandarqiuqiu\.com	Berhasil Terblokir
Game Online	*Mobile Legend*	Berhasil Terblokir
	PUBG Mobile	Berhasil Terblokir
	Free Fire	Berhasil Terblokir

c. Pengujian Keberhasilan Pembaruan *Regex* Otomatis

Memastikan bahwa sistem mencatat pembaruan *regex* berhasil dengan memeriksa log aktivitas. Log ini akan memberikan informasi terkait waktu pembaruan, status keberhasilan, serta kemungkinan adanya kesalahan selama proses pembaruan. Dengan memeriksa log, admin dapat

mengonfirmasi apakah pembaruan dilakukan sesuai jadwal dan apakah file *regex* telah diperbarui dengan benar tanpa adanya masalah teknis. Log aktivitas pembaruan *regex* seperti Gambar 9.



Gambar 9. Log Aktivitas Pembaruan *Regex*

d. Pengukuran Volume *Traffic*

Sebagai seorang admin jaringan, penting untuk memastikan bahwa lalu lintas jaringan berjalan sesuai dengan yang diharapkan. Salah satu cara untuk melakukannya adalah dengan menggunakan fitur graphing pada *mikrotik* untuk memantau lalu lintas jaringan. Perbandingan statistik *traffic* pada *interface <ether2>* sebelum dan sesudah implementasi web *filtering* seperti pada Tabel 6.

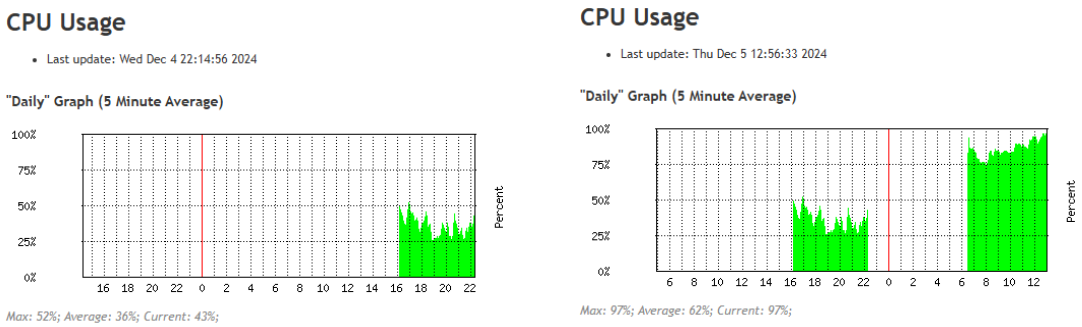
Tabel 6. Hasil MonitoringVolume *Traffic*

Parameter	Sebelum Implementasi	Sesudah Implementasi	Perubahan
Max In (Daily)	*20.38 Mb*	*1.29 Mb*	Penurunan signifikan
Average In (Daily)	*633.89 Kb*	*391.30 Kb*	Penurunan moderat
Current In (Daily)	*117.88 Kb*	*148.68 Kb*	Peningkatan kecil
Max Out (Daily)	*29.85 Mb*	*9.88 Mb*	Penurunan signifikan
Average Out (Daily)	*4.16 Mb*	*3.32 Mb*	Penurunan moderat
Current Out (Daily)	*1.54 Mb*	*456.48 Kb*	Penurunan drastis

Secara umum, setelah implementasi *web filtering*, *traffic inbound* dan *outbound* mengalami penurunan yang signifikan. Penurunan ini mencerminkan efektivitas dari web *filtering* dalam memblokir akses ke situs atau aktivitas yang tidak relevan, sehingga penggunaan *bandwidth* menjadi lebih terfokus pada kebutuhan yang prioritas. Dengan demikian, implementasi web *filtering* terbukti mampu mengoptimalkan jaringan dengan mengurangi beban *bandwidth* yang sebelumnya digunakan untuk aktivitas yang tidak produktif. Hal ini berkontribusi pada efisiensi jaringan secara keseluruhan.

e. Monitoring Sumber Daya Sistem *(CPU dan Memory)*

Monitoring penggunaan CPU dan *Memory* sebelum dan sesudah implementasi web filtering pada perangkat jaringan *mikrotik* penting untuk memahami dampak dari konfigurasi tersebut terhadap kinerja perangkat. Dalam penelitiannya, penulis melakukan *monitoring* CPU dan *Memory* selama 6 jam, baik sebelum maupun setelah implementasi dilakukan. Hasil monitoring penggunaan CPU seperti Gambar 10.



(a) (b)

Gambar 10. Hasil Monitoring Penggunaan CPU Sebelum *Filtering* (a), Setelah *Filtering* (b)

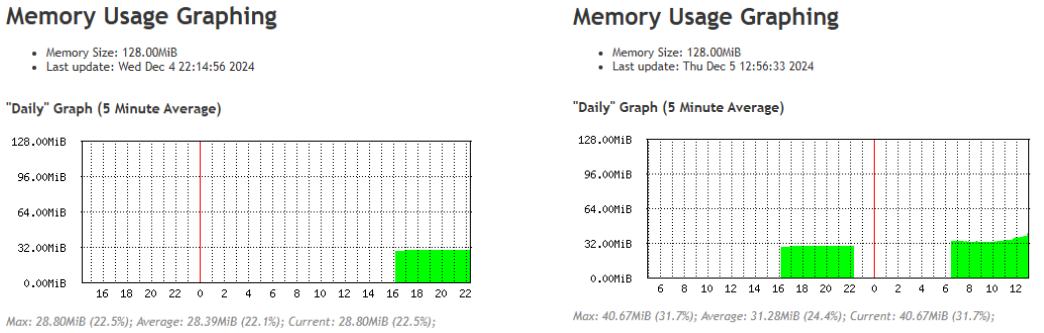
Analisis perbandingan penggunaan CPU sebelum dan setelah implementasi *web filtering* dilakukan untuk mengidentifikasi peningkatan beban kerja pada perangkat. Hasil analisis penggunaan CPU seperti pada Tabel 7.

Tabel 7. Hasil Monitoring CPU

Parameter	Sebelum *Filtering* (%)	Setelah *Filtering* (%)	Kenaikan (%)
Average	36%	62%	26%
Max	52%	97%	45%

Setelah implementasi *web filtering*, terjadi peningkatan penggunaan CPU rata-rata sebesar 26%. Peningkatan ini disebabkan oleh pemrosesan tambahan yang dibutuhkan, terutama pada *filtering* berbasis *Layer 7 protocol*, di mana setiap paket data yang melewati *firewall* harus dianalisis secara mendalam sesuai dengan aturan yang diterapkan.

Dalam jaringan, *monitoring* penggunaan memori perangkat *firewall* sangat penting untuk memastikan kinerja optimal, terutama saat fitur seperti *web filtering* diaktifkan. Hasil *monitoring* penggunaan memori seperti Gambar 11.



(a) (b)

Gambar 11. Hasil *Monitoring* Penggunaan Memori Sebelum *Filtering* (a), Setelah *Filtering* (b)

Analisis perbandingan penggunaan memori sebelum dan setelah implementasi web *filtering* dilakukan untuk mengidentifikasi peningkatan beban kerja pada perangkat. Hasil analisis penggunaan memori seperti Tabel 8.

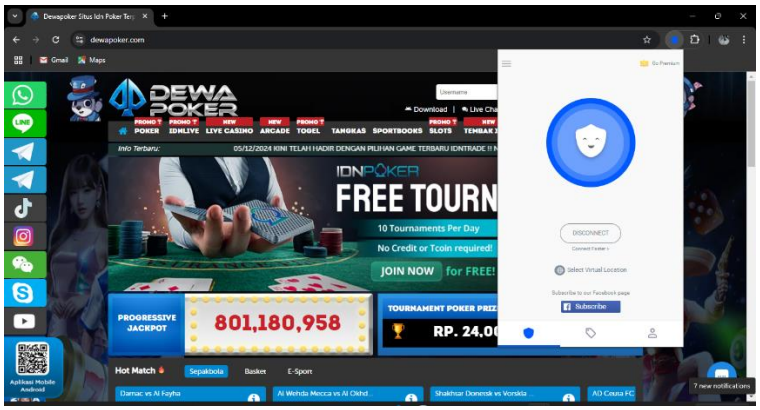
Tabel 8. Hasil *Monitoring* Memori

Parameter	Sebelum *Filtering* MiB(%)	Setelah *Filtering* MiB(%)	Kenaikan MiB(%)
Average	28.39Mib (22.1%)	31.28Mib (24.4%)	2.89Mib (2.3%)
Max	28.80Mib (22.5%)	40.67Mib (31.7%)	11,87Mib (9,2%)

Setelah implementasi *web filtering*, penggunaan memori meningkat rata-rata sebesar 2.89Mib/(2.3%). Peningkatan ini disebabkan oleh kebutuhan memori tambahan untuk menjalankan filtering berbasis *Layer 7 Protocol*, yang berfungsi menyimpan *cache*, tabel aturan, serta melakukan analisis pola trafik secara *real-time*. Jika penggunaan memori mendekati kapasitas maksimum perangkat, hal ini dapat berdampak negatif pada kinerja *firewall*, seperti penundaan dalam pemrosesan paket data atau bahkan kegagalan sistem yang dapat mengganggu stabilitas jaringan.

f. Pengujian dengan VPN

Pengujian akses jaringan yang telah dikonfigurasi dengan web *filtering* dilakukan untuk memastikan efektivitas pembatasan terhadap situs atau layanan tertentu. Pengujian ini dilakukan dengan mencoba mengakses situs yang diblokir langsung melalui jaringan internal, di mana akses tersebut berhasil dicegah sesuai dengan aturan web *filtering* yang diterapkan. Namun, ketika pengujian dilakukan menggunakan VPN eksternal, situs yang sebelumnya diblokir dapat diakses tanpa kendala. Hal ini menunjukkan bahwa web *filtering* berfungsi sesuai konfigurasi pada jaringan internal, tetapi dapat dilewati dengan penggunaan VPN eksternal yang menyembunyikan alamat IP pengguna dan mengenkripsi lalu lintas data, sehingga tidak terdeteksi oleh *firewall* internal. Hasil pengujian dengan menggunakan VPN seperti pada Gambar 12.



Gambar 12. Pengujian Akses Menggunakan VPN

3.5 Pemeliharaan

Pemeliharaan sistem merupakan bagian penting dalam menjaga efektivitas dan keberlanjutan dari konfigurasi yang telah dilakukan. Untuk memastikan sistem pemblokiran situs tetap berfungsi dengan baik, beberapa langkah pemeliharaan yang perlu dilakukan antara lain:

a. Pengecekan Kinerja *Mikrotik*

Pengecekan berkala sangat penting untuk memastikan efektivitas sistem *filtering*, sehingga disarankan untuk menjadwalkan pemeriksaan log dan evaluasi aturan filtering setiap minggu atau sesuai kebutuhan. Administrator dapat menggunakan alat *monitoring* yang tersedia di *mikrotik* untuk memeriksa penggunaan CPU dan memori. Jika ditemukan bahwa kinerja router menurun, bisa mempertimbangkan untuk mengoptimalkan *regex* yang digunakan atau meningkatkan kapasitas perangkat *mikrotik.* Selain itu, administrator harus selalu melakukan *backup* konfigurasi *mikrotik* sebelum dan sesudah melakukan perubahan untuk mencegah kehilangan data konfigurasi.

b. Pembaruan Otomatis *Regex*

Administrator perlu memeriksa log aktivitas untuk memastikan pembaruan *regex* berjalan sesuai jadwal dan mencatat hasilnya sebagai proses yang berhasil. Jika ditemukan kegagalan, penyebabnya harus segera diidentifikasi, seperti masalah konektivitas atau file yang korup. *Regex* yang ada perlu dievaluasi secara berkala untuk memastikan relevansinya terhadap ancaman baru.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Berdasarkan dari penelitian yang telah dilakukan, dapat disimpulkan bahwa web *filtering firewall* dapat melakukan pemblokiran akses pada beberapa situs pornografi, judi *online* dan *game online.* Melalui pemblokiran berbasis *layer 7 protocols dan regex* serta penggunaan *firewall*, penelitian ini membuktikan bahwa akses ke situs-situs tersebut dapat dibatasi secara efektif, sehingga menciptakan lingkungan internet yang aman dan sesuai dengan nilai-nilai pendidikan yang dianut di pesantren.

4.2 Saran

Dengan mempertimbangkan keterbatasan waktu dan pengetahuan yang dimiliki oleh peneliti, pengembangan lebih lanjut di masa mendatang sangat diperlukan. Beberapa saran untuk pengembangan tersebut adalah sebagai berikut:

a. Menjadwalkan *filtering* otomatis berdasarkan kebutuhan untuk mengoptimalkan penggunaan CPU dan memori. *Filtering* dapat diaktifkan pada jam aktif dan dikurangi atau dimatikan pada jam non-aktif, sehingga beban CPU dan memori lebih ringan.
b. Untuk meningkatkan efektivitas web *filtering,* disarankan untuk mengintegrasikan sistem dengan teknologi pendeteksi dan pemblokir VPN *(VPN detection and blocking).*
c. Memastikan bahwa penerapan pembatasan akses internet tidak hanya sebatas memblokir akses yang tidak diinginkan, akan tetapi juga harus diiringi dengan upaya meningkatkan kesadaran tentang pentingnya penggunaan internet secara bertanggung jawab untuk mendorong terbentuknya perilaku positif dalam penggunaan internet, sekaligus menciptakan lingkungan pesantren yang aman, produktif, dan beretika di era digital saat ini.

DAFTAR PUSTAKA

[1] M. A. Rozan *et al.*, "Implementasi Web Proxy Pada Mikrotik Untuk Mengoptimalkan Keamanan Jaringan Wireless Lan Di Lingkungan Sekolah MAN 1 Gesik," *Jurnal Pendidikan Teknologi Informasi (JUKANTI)*, vol. 7, no. 1, pp. 180–188, 2024.

[2] R. N. Dasmen, M. D. Nugraha, and Adelia, "Penerapan Pembatasan User Wi-Fi Pada Kantor Yayasan Patra Mandiri 01 Palembang," *Jurnal Komputer dan Informatika*, vol. 10, no. 1, pp. 18–23, 2022.

[3] M. Ilham, I. Gunawan, and Z. A. Siregar, "Keamanan Jaringan WLAN dengan Metode Firewall Filtering Menggunakan Mikrotik pada SMP Negeri 1 Dolok Merawan," *Jurnal Ilmiah Sistem Informasi dan Ilmu Komputer*, vol. 2, no. 3, pp. 1–16, 2022.

[4] A. Apriyanto, E. T. Alawiyah, and M. B. R. Mubaraq, "Perancangan Program Pengajuan Pemasangan Wifi Publik Kota Depok Berbasis Web," *Jurnal SIMADA (Sistem Informasi dan Manajemen Basis Data)*, vol. 4, no. 2, pp. 79–91, 2021.

[5] A. Majid, "Prototipe Manajemen Keamanan Jaringan di Pesantren (Study Kasus Pesantren Madinatunnajah)," *Walisongo Journal of Information Technology*, vol. 3, no. 1, pp. 29–42, Jul. 2021.

[6] Suparmadi, Akmal, Z. Sirait, and S. Gusti, "Penyuluhan Tentang Pemanfaatan Internet yang Aman dan Baik Bagi Santri Pondok Pesantren Mas Bahrul Uluum Al Kamal Asahan," *Jurnal Pemberdayaan Sosial dan Teknologi Masyarakat*, vol. 2, no. 2, pp. 187–192, 2023.

[7] Yuswardi *et al.*, "Program Internet Sehat Dan Aman Melalui Implementasi Bahan Ajar Digital Dan Video Edukasi Di Sekolah," *National Conference of Community Service Project*, vol. 4, no. 1, pp. 217–224, 2022.

[8] I. P. Saputra, R. Yusuf, and U. Saprudin, "Implementasi Cloud Computing Sebagai Radius Server Pada Jaringan Internet Router Mikrotik," *Journal Computer Science and Informatic Systems: J-Cosys*, vol. 1, no. 2 pp.81-86, 2021.

[9] A. S. Amin, K. Harsanto, and R. Samsinar, "Implementasi Jaringan Kabel dan Wireless Menggunakan Router Mikrotik pada SD Muhammadiyah 1 Jakarta," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 5, no. 2, pp. 255–264, 2022.
[10] A. Jamalul'ain, O. Nurdiawan, and M. Martanto, "Optimalisasi Keamanan Jaringan Komputer Menggunakan Metode Knocking Port Berbasis Mikrotik (Studi Kasus: CV. Mitra Indexindo Pratama)," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 6, no. 2, pp. 560–570, 2022.
[11] A. B. Pratomo, "Pengembangan Sistem Firewall Pada Jaringan Komputer Berbasis Mikrotik Routeros," *Bulletin of Network Engineer and Informatics*, vol. 1, no. 2, pp. 51–59, 2023.
[12] A. Syaripudin and A. Nugraha, "Analisa Dan Implementasi Blocking Website Dengan Metode 7 Layer Pada Perangkat Mikrotik Di Garage Freshmart," *Jurnal Informatika MULTI*, vol. 1, no. 4, pp. 447–455, 2023.
[13] H. Haryanto, R. D. Rahmah, and A. P. Sari, "Implementasi Web Proxy Menggunakan Router Mikrotik Pada Kantor Suku Dinas Walikota Administrasi Jakarta Barat," *JIKA (Jurnal Informatika)*, vol. 5, no. 3, pp. 298–306, 2021.
[14] D. Sukma and S. S. Mitro, "Penerapan Internet Positif Di SMK N 3 Pandeglang Berbasis Mikrotik Dengan Packet Filtering," *Jurnal POLEKTRO: Jurnal Power Elektronik*, vol. 12, no. 3, pp. 188–191, 2023.
[15] M. Ali and F. Latifah, "Implementasi Block Access Pengguna Layanan Internet Dengan Metode Filter Rule dan Layer 7 Protocol," *Journal of Information System, Applied, Management, Accounting and Research*, vol. 5, no. 2, pp. 340–349, 2021.
[16] B. Santosa and A. A. Rismayadi, "Implementasi Keamanan Jaringan Lan Menggunakan Mikrotik Dengan Metode Firewall Filtering," *eProsiding Teknik Informatika*, vol. 3, no. 1, pp. 179–190, 2022.
[17] C. K. Wilujeng and A. Voutama, "Implementasi Firewall Filter Rules Sebagai Filtering Content Pada Jaringan Komputer Menggunakan Mikrotik," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 3, pp. 2680–2685, 2024.