

IMPLEMENTASI WEB PROXY FILTERING BERBASIS MIKROTIK UNTUK PENGUATAN KEAMANAN JARINGAN DAN PENCEGAHAN AKSES SITUS JUDI ONLINE DI KAMPUS UNUSIDA

Dwi Ira Fuji Antika, Mochammad Machlul Alamin

Informatika, Universitas Nahdlatul Ulama Sidoarjo

Jalan Lingkar Timur KM 5,5 Rangkah Kidul Sidoarjo, Indonesia

dwiirafuji23@gmail.com, machlul410.tif@unusida.ac.id

ABSTRAK

Perkembangan teknologi jaringan komputer yang pesat menjadikan internet sebagai sarana utama dalam mendukung aktivitas pendidikan, namun juga menimbulkan permasalahan berupa meningkatnya akses ke situs bermuatan negatif seperti judi online yang dapat mengganggu etika dan produktivitas mahasiswa. Permasalahan utama dalam jaringan Kampus Universitas Nahdlatul Ulama Sidoarjo (UNUSIDA) adalah belum adanya sistem penyaringan konten yang mampu mencegah akses ke situs judi online secara efektif. Penelitian ini bertujuan untuk mengimplementasikan web proxy filtering berbasis Mikrotik sebagai solusi dalam meningkatkan keamanan jaringan serta mendukung terciptanya internet sehat di lingkungan kampus. Metode penelitian meliputi analisis sistem jaringan yang ada, perancangan topologi dan konfigurasi web proxy, hingga tahap implementasi dan pengujian menggunakan mode transparent proxy agar seluruh aktivitas pengguna disaring otomatis tanpa konfigurasi manual. Hasil pengujian menunjukkan bahwa implementasi web proxy filtering berhasil memblokir 100% dari 50 sampel situs judi online yang diuji. Sistem ini terbukti efektif dalam membatasi akses konten negatif tanpa menurunkan performa akses ke situs akademik kampus, sehingga menciptakan lingkungan internet yang lebih sehat dan aman di UNUSIDA.

Kata kunci : Mikrotik, Web Proxy, Filtering, Judi Online, UNUSIDA.

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer saat ini mengalami kemajuan yang sangat pesat, menjadikan internet sebagai sarana utama dalam memperoleh informasi secara cepat dan efisien. Namun, di balik manfaatnya, kemudahan akses internet juga menimbulkan berbagai permasalahan, salah satunya adalah meningkatnya akses terhadap situs bermuatan negatif seperti pornografi, kekerasan, dan perjudian (*online gambling*). Kondisi ini menimbulkan kekhawatiran, terutama di lingkungan akademik, karena dapat memengaruhi moral, produktivitas, serta konsentrasi mahasiswa dalam proses pembelajaran [1].

Permasalahan utama yang dihadapi di Kampus Universitas Nahdlatul Ulama Sidoarjo (UNUSIDA) adalah belum tersedianya sistem penyaringan konten (*content filtering system*) yang mampu mengontrol dan membatasi akses pengguna terhadap situs-situs terlarang secara efektif. Akibatnya, lalu lintas jaringan tidak terpantau dengan baik, dan risiko penyalahgunaan koneksi internet menjadi tinggi. Hal ini menunjukkan perlunya solusi teknis yang dapat meningkatkan keamanan jaringan sekaligus menjaga lingkungan digital yang sehat [2].

Salah satu solusi yang dapat diterapkan adalah penggunaan web proxy filtering berbasis Mikrotik. Teknologi ini berfungsi sebagai perantara antara klien dan server untuk mengatur lalu lintas data serta melakukan pemblokiran otomatis terhadap situs yang masuk dalam daftar *blacklist*. Penerapan web proxy filtering berbasis Mikrotik memungkinkan administrator jaringan untuk mengawasi aktivitas

pengguna, membatasi akses ke situs negatif, dan memastikan bandwidth digunakan secara efisien untuk kebutuhan akademik [3].

Selain dari sisi teknis, urgensi penerapan sistem penyaring konten juga sejalan dengan nilai-nilai Islam yang menekankan pentingnya menjauhi perbuatan merugikan seperti perjudian. Dalam Al-Qur'an, Allah SWT melarang praktik judi sebagaimana tertulis dalam QS. Al-Maidah ayat 90, yang menjelaskan bahwa berjudi termasuk perbuatan keji dari setan dan wajib di jauhi. Oleh karena itu, implementasi web proxy filtering berbasis Mikrotik di lingkungan Kampus UNUSIDA tidak hanya memiliki nilai teknologi dalam memperkuat keamanan jaringan, tetapi juga nilai religius dalam mendukung terciptanya lingkungan akademik yang sehat, produktif, dan sesuai dengan tuntunan syariat Islam.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terkait

Beberapa penelitian sebelumnya telah membahas penerapan web proxy filtering berbasis Mikrotik sebagai solusi untuk meningkatkan keamanan jaringan serta mengendalikan akses terhadap konten negatif di lingkungan pendidikan. Penelitian oleh Syaiful dan Doni [4] membahas penerapan router Mikrotik RB941-2nD dengan konfigurasi web proxy untuk memblokir situs negatif seperti pornografi dan judi online. Hasil pengujian menunjukkan bahwa seluruh access point berhasil memblokir domain terlarang, sehingga sistem dinilai efektif dalam menciptakan lingkungan internet yang sehat dan membantu pengawasan penggunaan jaringan di sekolah.

Selanjutnya, Riki Yakub dkk. [5] menerapkan web proxy pada Mikrotik untuk meningkatkan keamanan jaringan nirkabel di SMP Negeri 1 Labang. Sistem ini mampu memblokir konten tidak relevan secara otomatis tanpa konfigurasi tambahan pada pengguna, sehingga mendukung disiplin penggunaan internet serta meningkatkan efisiensi jaringan di lingkungan pendidikan.

Penelitian oleh Rifqi dan Hendra [6] juga menunjukkan bahwa kombinasi fitur web proxy dan firewall NAT pada Mikrotik RB941-2ND-TC efektif dalam memblokir situs judi online. Hasil uji coba membuktikan keberhasilan pemblokiran pada komputer dan smartphone, menjadikan Mikrotik solusi andal untuk menciptakan jaringan yang aman, sehat, dan terkendali.

2.2. Keamanan Jaringan

Keamanan jaringan merupakan elemen penting dalam pengelolaan sistem informasi modern yang berfungsi melindungi data dan infrastruktur dari berbagai ancaman yang dapat mengganggu kelancaran operasional sistem. Seiring perkembangan teknologi informasi yang pesat, ketergantungan organisasi terhadap jaringan komputer untuk komunikasi, penyimpanan data, dan layanan digital semakin tinggi. Kondisi ini memperbesar potensi ancaman, baik dari sisi fisik seperti kerusakan perangkat keras, maupun dari sisi logis seperti peretasan (*hacking*) dan pencurian data. Oleh karena itu, diperlukan mekanisme perlindungan yang komprehensif guna menjaga keamanan dan keandalan sistem [7].



Gambar 1. Keamanan Jaringan

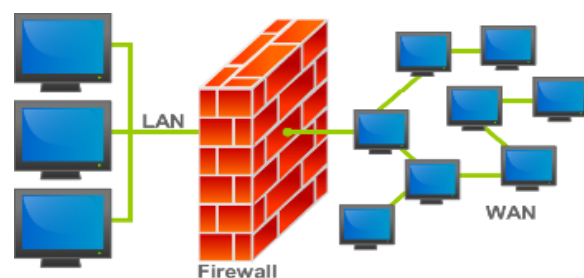
Keamanan jaringan bertujuan mencegah serta mendeteksi akses tidak sah terhadap sistem komputer, dengan menekankan empat aspek utama, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), keaslian (*authenticity*), dan ketersediaan (*availability*). Keempat aspek ini menjadi dasar dalam menjaga keandalan sistem informasi agar tetap berfungsi optimal. Menurut penelitian Khairul Aziz dkk. [8] dalam studi Implementasi Keamanan Jaringan dengan Metode Firewall Filtering Menggunakan Mikrotik di SMKN 3 Payakumbuh, penerapan prinsip keamanan jaringan melalui konfigurasi firewall pada Mikrotik terbukti mampu melindungi sistem dari akses tidak sah dan serangan jaringan. Dengan demikian, pemahaman

dan penerapan keamanan jaringan menjadi aspek fundamental tidak hanya bagi sektor bisnis, tetapi juga bagi dunia pendidikan dan pemerintahan dalam mewujudkan sistem informasi yang aman, andal, dan berkelanjutan.

2.3. Firewall dan Filtering Web

Firewall jaringan merupakan salah satu komponen vital dalam sistem keamanan jaringan modern yang berfungsi mengontrol dan mengawasi lalu lintas data antara jaringan internal dan jaringan eksternal. Mekanisme kerja firewall didasarkan pada penerapan aturan atau kebijakan keamanan tertentu untuk menentukan apakah suatu paket data diperbolehkan melintas atau harus diblokir, dengan mempertimbangkan parameter seperti alamat sumber, tujuan, port, serta jenis protokol yang digunakan [9]. Dalam lingkungan jaringan kampus, firewall tidak hanya berperan sebagai penghalang terhadap ancaman dari luar, tetapi juga sebagai alat pengendali aktivitas pengguna internal agar tetap selaras dengan kebijakan penggunaan jaringan yang telah ditetapkan.

Selain fungsi perlindungan, firewall juga memiliki peran penting dalam mendukung penerapan web filtering atau penyaringan akses internet. Melalui fitur content filtering, administrator jaringan dapat membatasi atau menolak akses ke situs dan layanan tertentu berdasarkan kategori konten, alamat IP, URL, maupun jenis protokol komunikasi. Kebijakan ini sangat relevan untuk mencegah akses ke konten negatif seperti perjudian online, pornografi, dan kekerasan yang berpotensi mengganggu proses belajar mengajar serta etika akademik. Proses penyaringan dapat diterapkan pada berbagai lapisan jaringan, mulai dari network layer hingga application layer, sehingga memberikan fleksibilitas dan efektivitas dalam pengamanan jaringan [10].



Gambar 2. Firewall

Selain itu, penerapan firewall dan web filtering yang terintegrasi juga berkontribusi dalam meningkatkan kinerja dan stabilitas jaringan kampus. Dengan membatasi akses ke situs yang tidak relevan atau berisiko tinggi, penggunaan bandwidth dapat dioptimalkan untuk kegiatan akademik dan administratif yang lebih prioritas [11]. Di sisi lain, sistem ini membantu administrator jaringan dalam melakukan pemantauan, pencatatan (*logging*), serta evaluasi aktivitas jaringan secara berkelanjutan. Oleh karena itu, firewall dan web filtering tidak hanya

berfungsi sebagai alat keamanan, tetapi juga sebagai sarana manajemen jaringan yang mendukung terciptanya lingkungan digital yang aman, tertib, dan kondusif di institusi pendidikan.

2.4. Web Proxy Filtering

Web proxy merupakan layanan perantara antara pengguna dan internet yang berfungsi mengatur, memantau, dan mengendalikan lalu lintas akses web, sedangkan filtering adalah proses penyaringan akses berdasarkan aturan tertentu untuk membatasi atau memblokir situs yang tidak diizinkan. Dengan menggabungkan web proxy dan filtering, administrator jaringan dapat meningkatkan keamanan jaringan, mengawasi aktivitas pengguna, serta mencegah akses ke situs berbahaya seperti situs judi online sesuai dengan kebijakan yang telah ditetapkan.

Web proxy filtering merupakan mekanisme pengendalian akses internet yang berfungsi sebagai perantara antara pengguna (*client*) dan server tujuan. Sistem ini memeriksa serta memfilter setiap permintaan akses sebelum diteruskan ke server, sehingga administrator dapat mengatur kebijakan seperti pemblokiran situs berkonten negatif, pengelolaan hak akses, dan pencatatan aktivitas jaringan [12]. Teknologi ini tidak hanya berperan sebagai alat penyaring konten, tetapi juga sebagai sistem pengelolaan jaringan yang meningkatkan keamanan, efisiensi, dan kecepatan akses internet.

Fungsi utama web proxy filtering adalah menyaring lalu lintas data berdasarkan kriteria tertentu, seperti memblokir situs perjudian, pornografi, atau media sosial yang tidak relevan dengan aktivitas akademik. Selain itu, fitur caching pada web proxy membantu menghemat bandwidth dengan menyimpan data sementara dari situs yang sering diakses, sehingga akses berikutnya menjadi lebih cepat dan efisien [13].



Gambar 3. Web Proxy Filtering

Dalam konteks keamanan jaringan, penerapan web proxy filtering berbasis Mikrotik dianggap sebagai solusi efektif karena menyediakan konfigurasi yang fleksibel dan mudah digunakan. Berdasarkan penelitian Ma'mun [14], Mikrotik memungkinkan administrator jaringan untuk mengontrol situs yang dapat diakses dan memantau aktivitas pengguna secara real time, sehingga menciptakan lingkungan internet yang aman, terkendali, serta mendukung proses pembelajaran yang sehat di lingkungan kampus maupun sekolah [15].

2.5. UNUSIDA

Universitas Nahdlatul Ulama Sidoarjo (UNUSIDA) merupakan perguruan tinggi swasta di bawah naungan organisasi Islam terbesar di Indonesia, Nahdlatul Ulama. Berdiri dengan landasan nilai keislaman, kebangsaan, dan keilmuan, UNUSIDA berkomitmen untuk mencetak lulusan yang berkompeten, berakhlak mulia, serta siap berkontribusi dalam pembangunan masyarakat. Sebagai lembaga pendidikan tinggi, UNUSIDA menyelenggarakan berbagai program studi yang mencakup rumpun ilmu sains, teknologi, sosial, dan humaniora, yang seluruhnya diarahkan untuk menjawab tantangan perkembangan zaman.

Fakultas Ilmu Komputer menjadi salah satu pilar penting dalam pengembangan riset dan teknologi di lingkungan kampus. Melalui tenaga pendidik profesional, sarana pembelajaran modern, dan suasana akademik yang kondusif, universitas ini berupaya menghasilkan sumber daya manusia yang unggul serta mampu bersaing di tingkat nasional maupun global.



Gambar 4. UNUSIDA

3. METODE PENELITIAN

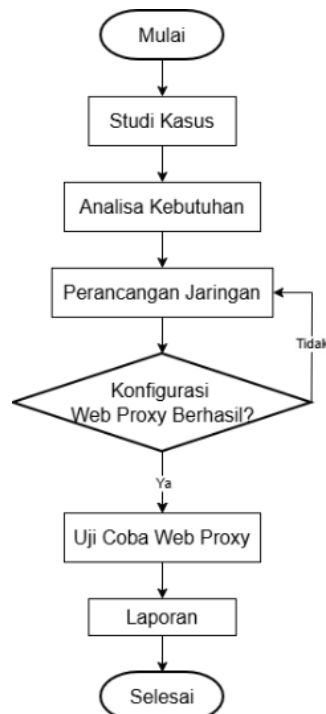
3.1. Diagram Rancangan Penelitian

Diagram rancangan penelitian pada implementasi Web Proxy Filtering berbasis Mikrotik di Kampus UNUSIDA berfungsi untuk menggambarkan alur dan tahapan penelitian secara menyeluruh, mulai dari identifikasi masalah hingga pengujian sistem. Diagram ini membantu menjelaskan proses penelitian yang sistematis dalam upaya memperkuat keamanan jaringan serta mencegah akses ke situs judi online sesuai dengan kebijakan institusi.

Tahap awal penelitian diawali dengan identifikasi permasalahan dan analisis kebutuhan jaringan melalui pengamatan kondisi jaringan eksisting di lingkungan kampus. Hasil analisis ini digunakan sebagai dasar perancangan sistem jaringan berbasis Mikrotik, yang meliputi desain konfigurasi web proxy, penentuan daftar situs yang diblokir (blacklist), pengaturan firewall, serta perancangan topologi jaringan agar penerapan sistem dapat berjalan secara efektif dan terstruktur.

Tahap selanjutnya adalah implementasi dan pengujian sistem, di mana rancangan yang telah dibuat diterapkan pada perangkat Mikrotik dan diintegrasikan

dengan jaringan kampus. Pengujian dan evaluasi dilakukan untuk menilai efektivitas penyaringan situs judi online serta dampaknya terhadap kinerja jaringan. Evaluasi ini bertujuan untuk mengetahui peningkatan keamanan dan stabilitas jaringan setelah penerapan web proxy filtering di Kampus UNUSIDA.



Gambar 5. Diagram Rancangan Penelitian

3.2. Analisis Kebutuhan

Penerapan Web Proxy Filtering berbasis Mikrotik di Kampus UNUSIDA membutuhkan dukungan perangkat keras dan perangkat lunak untuk menjamin keamanan serta kelancaran operasional jaringan. Perangkat keras yang digunakan terdiri dari router Mikrotik sebagai pengendali utama jaringan, switch sebagai penghubung antar perangkat, dan komputer atau laptop sebagai perangkat pengguna. Adapun perangkat lunak yang digunakan meliputi RouterOS untuk konfigurasi web proxy, firewall, dan pemblokiran situs judi online, serta Winbox untuk memudahkan proses pengelolaan dan pemantauan jaringan.

Berikut adalah perangkat lunak dan perangkat keras yang digunakan dalam penelitian ini :

Tabel 1. Kebutuhan Perangkat Keras

No	Prangkat Keras	Tipe	Keterangan
1.	Router Mikrotik	RB941-2nD	Mengelola koneksi jaringan
2.	Kabel LAN	7814A Belden	Menghubungkan perangkat keras
3.	Laptop	Asus Amd Ryzen 5	Perangkat client/server

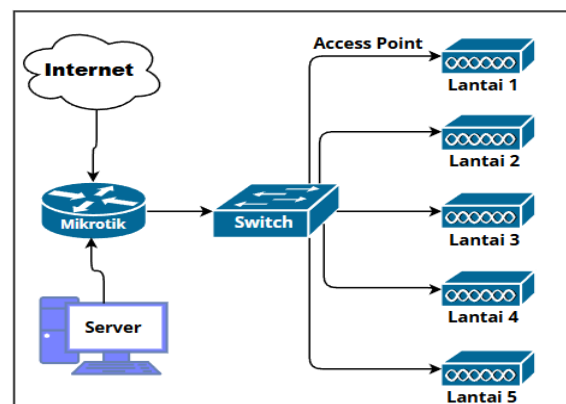
Tabel 2. Kebutuhan Perangkat Lunak

No	Perangkat Lunak	Tipe
1.	RouterOS	Level 4
2.	Winbox	Winbox 64 bit
3.	Windows	Windows 11

3.3. Skema Jaringan

Skema jaringan merupakan gambaran struktur dan alur koneksi antarperangkat yang digunakan untuk menjelaskan mekanisme kerja sistem Web Proxy Filtering berbasis Mikrotik dalam meningkatkan keamanan jaringan dan mencegah akses ke situs judi online di Kampus UNUSIDA. Skema ini berfungsi untuk memperlihatkan hubungan antarperangkat jaringan sekaligus menjadi acuan dalam analisis serta penanganan masalah apabila terjadi gangguan pada proses penyaringan lalu lintas internet.

Skema jaringan yang diterapkan terdiri dari router Mikrotik sebagai pusat pengendali lalu lintas data, switch sebagai penghubung antarperangkat, dan komputer klien sebagai pengguna jaringan. Seluruh permintaan akses internet dari pengguna diarahkan melalui Mikrotik untuk dilakukan proses filtering sebelum diteruskan ke jaringan luar, sehingga situs judi online dan situs berbahaya lainnya dapat diblokir secara otomatis. Skema ini dirancang dengan mempertimbangkan keamanan, efisiensi, dan kestabilan koneksi agar mendukung aktivitas akademik civitas UNUSIDA secara optimal.



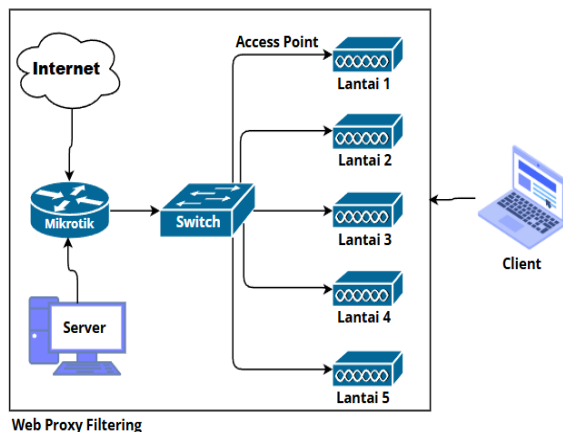
Gambar 6. Skema Jaringan UNUSIDA

3.4. Skema Topologi Web Proxy Filtering

Perancangan Web Proxy Filtering berbasis Mikrotik bertujuan untuk menyediakan sistem penyaringan akses internet yang aman dan efisien dalam menjaga keamanan jaringan kampus. Seluruh permintaan akses web dari pengguna diarahkan melalui proxy server sehingga aktivitas dapat difilter dan diawasi, memungkinkan pemblokiran otomatis terhadap situs berbahaya seperti situs judi online sebelum diteruskan ke internet.

Dalam perancangannya, Mikrotik dikonfigurasi sebagai proxy server utama dengan pengaturan jaringan dasar, aktivasi web proxy, dan pengalihan lalu lintas melalui firewall. Sistem dilengkapi dengan pengaturan blacklist dan whitelist serta diterapkan

dalam mode transparent proxy agar tidak memerlukan konfigurasi pada sisi klien. Untuk menjaga kinerja dan keamanan jaringan, dilakukan pemeliharaan berkala melalui pembaruan daftar situs, pemantauan lalu lintas, dan analisis log sehingga sistem tetap stabil dan efektif di lingkungan Kampus UNUSIDA. Pengujian dilakukan untuk memastikan aturan (rule) pada Mikrotik berjalan sesuai rencana. Skenario yang digunakan adalah:



Gambar 7. Skema Topologi UNUSIDA

Akses Situs Terlarang: Pengguna mencoba mengakses URL judi online yang ada dalam daftar

blacklist. Sistem diharapkan menampilkan halaman "403 Forbidden".

Akses Situs Akademik: Pengguna mengakses situs resmi kampus (unusida.ac.id) untuk memastikan proxy tidak memblokir trafik yang sah.

Verifikasi Log: Admin memeriksa menu Log dan Web Proxy Cache pada Winbox untuk melihat apakah trafik yang diblokir tercatat secara sistematis.

Data blokir website yang disajikan pada Tabel 3 merupakan daftar domain situs judi online yang digunakan sebagai objek pengujian dalam implementasi sistem penyaringan konten di lingkungan Kampus UNUSIDA. Daftar ini mencakup 50 alamat URL situs perjudian, seperti MIZUSLOT, MacauDewa, hingga HAJAR69, yang dikategorikan sebagai konten negatif yang dapat menghambat produktivitas serta melanggar etika akademik mahasiswa. Melalui penerapan Web Proxy Filtering berbasis Mikrotik, seluruh tautan tersebut dimasukkan ke dalam daftar hitam (blacklist) agar permintaan akses dari pengguna dapat dideteksi dan diblokir secara otomatis oleh sistem. Langkah ini bertujuan untuk memastikan keamanan jaringan serta mendukung terciptanya lingkungan digital yang sehat dan sesuai dengan nilai-nilai religius di Universitas Nahdlatul Ulama Sidoarjo.

Berikut adalah rincian data situs judi online yang digunakan dalam penelitian ini:

Tabel 3. Data Blokir Website

No	Link Website	Kategori	Status Akses	Hasil
1.	https://mizuslot.website/	Judi Online	Terblokir	403 Forbidden
2.	https://mc-dewa12.com/	Judi Online	Terblokir	403 Forbidden
3.	https://sv4.hokidewawin.com/	Judi Online	Terblokir	403 Forbidden
	... (dan 46 situs lainnya)	Judi Online	Terblokir	403 Forbidden
50.	https://injeksihajar.com/	Judi Online	Terblokir	403 Forbidden

Tabel 4. Rekap Persentase Keberhasilan

Kategori Pengujian	Jumlah Sampel	Berhasil	Gagal
Pemblokiran Situs Judol	50	50	0
Total	50	50	0

Berdasarkan Tabel 3 dan Tabel 4, dapat dianalisis bahwa Web Proxy Filtering yang diterapkan pada Mikrotik RB941-2nD mampu mengenali dan menghentikan request ke domain yang terdaftar dalam Access List dengan akurasi 100%. Pengujian juga membuktikan bahwa rule yang dibuat tidak bersifat over-blocking, di mana situs-situs produktif seperti website kampus dan mesin pencari tetap dapat diakses dengan normal.

4. HASIL DAN PEMBAHASAN

Dalam implementasi Web Proxy Filtering berbasis Mikrotik untuk pencegahan akses situs judi online, diperlukan serangkaian langkah yang harus diterapkan secara sistematis agar sistem penyaringan

yang dibangun dapat beroperasi dengan baik, stabil, dan memiliki tingkat keamanan jaringan yang optimal.

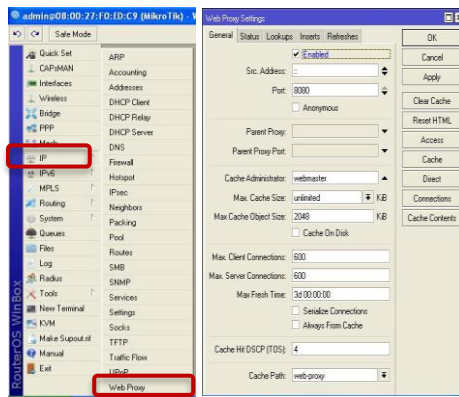
4.1. Tahap Konfigurasi

Setiap tahapan dalam proses ini harus dilakukan secara cermat, mulai dari persiapan perangkat keras dan perangkat lunak, konfigurasi web proxy dan firewall, hingga pengujian pemblokiran situs untuk memastikan bahwa sistem dapat berfungsi sesuai dengan tujuan yang diharapkan. Berikut adalah langkah-langkah konfigurasi yang harus dilakukan

4.2. Konfigurasi IP Web Proxy

Setelah berhasil login ke Winbox, langkah selanjutnya adalah mengaktifkan fitur Web Proxy dengan membuka menu IP → Web Proxy.

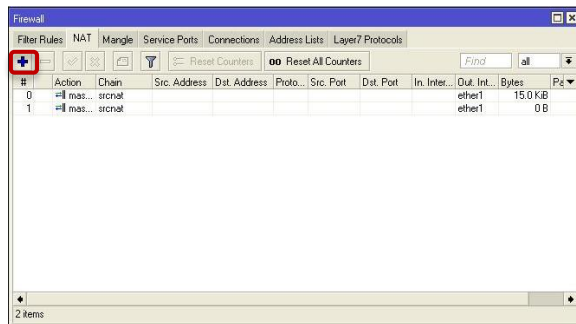
Pada menu ini, administrator mengaktifkan Web Proxy dengan mencentang opsi Enabled. Web Proxy berfungsi sebagai perantara antara client dan internet, sehingga seluruh permintaan akses website dapat dipantau dan difilter. Lalu mengatur port web proxy (default 8080) seperti pada gambar dibawah ini.



Gambar 8. Konfigurasi IP Web Proxy

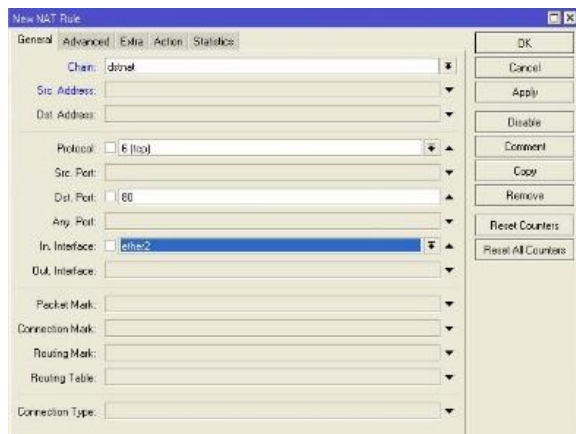
4.3. Konfigurasi IP Firewall

Langkah berikutnya adalah melakukan konfigurasi Firewall Filter Rules dengan membuka menu IP → Firewall → Filter Rules.



Gambar 9. Setting IP Firewall

Pada tahap ini, administrator menambahkan rule firewall untuk mengatur lalu lintas data yang masuk ke router. Firewall berfungsi sebagai sistem keamanan jaringan yang mengontrol paket data berdasarkan aturan tertentu, sehingga hanya trafik yang diizinkan saja yang dapat diproses oleh router. Seperti pada gambar dibawah ini, pada tahap ini, administrator mengatur chain dstnat dengan protocol TCP dan destination port 80 (HTTP) untuk mengalihkan trafik web dari client.



Gambar 10. Membuat NAT Rule baru

Rule NAT ini berfungsi untuk mengalihkan seluruh permintaan HTTP dari interface client (ether2) menuju layanan Web Proxy, sehingga Web Proxy dapat bekerja secara transparent tanpa perlu pengaturan manual pada browser client.

Pada tahap ini, administrator memilih action redirect dan menentukan To Ports 8080 sebagai port layanan Web Proxy. Konfigurasi ini berfungsi untuk mengalihkan seluruh trafik HTTP (port 80) yang berasal dari client ke port Web Proxy (8080) pada router Mikrotik, sehingga Web Proxy dapat bekerja secara transparent tanpa memerlukan konfigurasi tambahan pada sisi client.

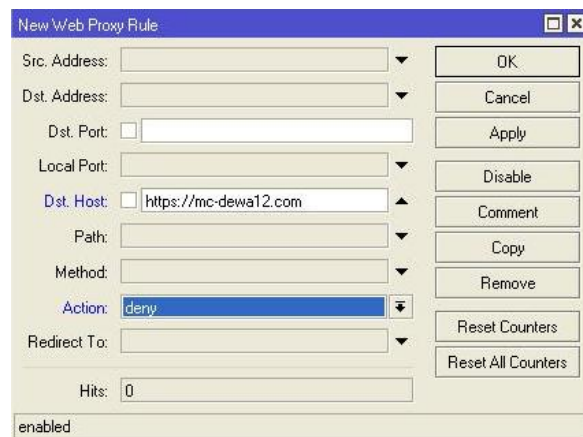


Gambar 11. Konfigurasi Action NAT Rule

4.4. Konfigurasi Web Proxy

Pada tahap ini, administrator menambahkan rule untuk memblokir akses ke situs tertentu dengan menentukan Destination Host (Dst. Host) yang akan dibatasi. Pada gambar dibawah ditunjukkan pengisian Dst. Host (<https://mc-dewa12.com>) dengan action deny, yang berarti setiap permintaan akses menuju alamat tersebut akan ditolak oleh Web Proxy.

Konfigurasi ini bertujuan untuk menerapkan kebijakan pembatasan akses internet, khususnya untuk mencegah pengguna mengakses situs yang tidak diizinkan, seperti situs judi online.

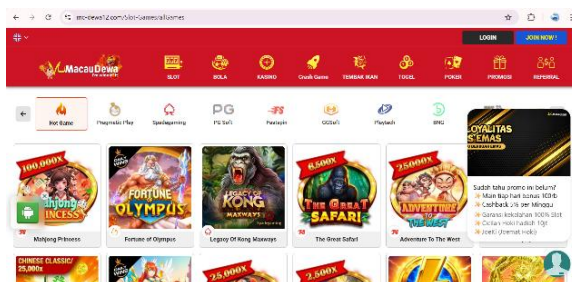


Gambar 12. Konfigurasi Web Proxy

4.5. Hasil Pengujian

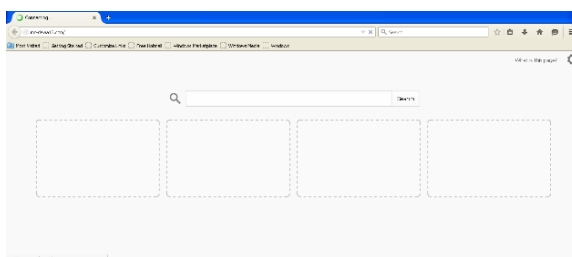
Selanjutnya, lakukan pengujian di sisi client dengan mengakses daftar situs judi online yang telah ditentukan melalui aplikasi peramban web (browser). Isikan alamat URL situs target pada bilah alamat, lalu sistem Web Proxy pada Mikrotik akan secara otomatis menyaring permintaan tersebut tanpa perlu konfigurasi tambahan pada perangkat pengguna. Setelah situs dipanggil, akses akan diblokir secara otomatis oleh sistem, dan jika konfigurasi berhasil, status pada layar akan berubah menjadi "403 Forbidden" atau "Access Denied" atau "Situs Tidak Ditemukan" yang menandakan bahwa konten tersebut telah berhasil disaring oleh kebijakan keamanan jaringan kampus.

Gambar di bawah ini memperlihatkan tampilan awal sebuah website judi online yang masih dapat diakses secara normal sebelum dilakukan proses pemblokiran. Website tersebut juga menampilkan elemen visual yang menarik, seperti banner promosi, daftar permainan unggulan, bonus, serta tombol navigasi seperti login dan daftar, yang bertujuan untuk menarik minat pengguna agar melakukan aktivitas perjudian secara daring.



Gambar 13. Tampilan Website Sebelum Diblokir

Kondisi ini menunjukkan bahwa sebelum pemblokiran diterapkan, akses ke website judi online tidak mengalami kendala, baik dari sisi konektivitas maupun tampilan konten. Gambar ini digunakan sebagai pembandingan untuk menunjukkan perbedaan kondisi sebelum dan sesudah penerapan pemblokiran website judi online dalam sistem jaringan yang diteliti.



Gambar 14. Tampilan Website Setelah Diblokir

Gambar di atas menunjukkan kondisi ketika sebuah website judi online berhasil diblokir oleh sistem jaringan atau mekanisme penyaringan akses internet. Pemblokiran ini ditandai dengan tampilan halaman yang tidak memuat konten secara normal, di mana situs terlihat terus melakukan proses loading tanpa menampilkan informasi apa pun, serta muncul

indikasi bahwa situs tidak dapat ditemukan (site not found). Berdasarkan pengujian terhadap 50 domain situs judi online yang berbeda, didapatkan hasil dengan jumlah situs diuji 50, yang berhasil diblokir 50, yang gagal diblokir 0, dengan persentase keberhasilan 100%.

Saat dilakukan akses ke situs terlarang, pada menu IP > Web Proxy > Hits di Winbox terlihat peningkatan jumlah hits yang menandakan bahwa request dari klien ditangkap oleh proxy dan langsung ditolak sesuai dengan Access Rule yang telah dibuat. Hal ini membuktikan bahwa beban kerja filter berada pada router, bukan pada perangkat pengguna.

Untuk memastikan sistem penyaringan berjalan dengan baik, pengguna dapat melakukan uji akses terhadap situs-situs terlarang melalui aplikasi peramban pada perangkat *client* yang terhubung ke jaringan kampus. Pada implementasi ini, dilakukan beberapa kali uji coba terhadap alamat URL yang berbeda-beda guna memastikan efektivitas pemblokiran oleh sistem *Web Proxy* pada Mikrotik. Hasil pengujian menunjukkan bahwa setiap upaya akses ke domain yang masuk dalam daftar hitam akan secara otomatis ditolak oleh *router*, sehingga pengguna tidak dapat menjangkau konten negatif tersebut dan keamanan jaringan di Kampus UNUSIDA tetap terjaga dengan optimal.

5. KESIMPULAN DAN SARAN

Implementasi Web Proxy Filtering berbasis Mikrotik di Kampus UNUSIDA terbukti efektif dalam meningkatkan keamanan jaringan dan mencegah akses terhadap konten negatif, khususnya situs judi online. Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa implementasi web proxy filtering berbasis Mikrotik di UNUSIDA memiliki tingkat keberhasilan sebesar 100% dalam memblokir 50 sampel situs judi online. Pengujian juga menunjukkan bahwa sistem transparent proxy yang diterapkan tidak mengganggu akses terhadap layanan publik dan akademik kampus, sehingga sangat layak digunakan sebagai standarisasi keamanan jaringan di lingkungan universitas. Meskipun sistem ini berhasil memblokir situs-situs yang telah terdaftar dalam blacklist, disarankan bagi administrator jaringan untuk melakukan pembaruan daftar URL secara berkala mengingat sangat cepatnya kemunculan domain judi online baru. Selain itu, pengembangan penelitian selanjutnya dapat mengombinasikan metode filtering ini dengan sistem Layer 7 Protocol atau penggunaan DNS filtering pihak ketiga untuk memberikan perlindungan yang lebih komprehensif terhadap ancaman siber dan konten negatif lainnya.

DAFTAR PUSTAKA

- [1] A. Yasin, "Implementasi DNS Filtering berbasis RPZ Menggunakan Databases DNSTrust Kominfo di PT. GN," Jurnal Ilmu Komputer (JUIK), vol. 4, no. 3, Oct. 2024.

- [2] A. E. Tangkowitz, V. R. Palilingan, and O. E. S. Liando, "Analisis dan Perancangan Jaringan Komputer di Sekolah Menengah Pertama," *EduTIK: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, vol. 1, no. 1, Feb. 2021.
- [3] A. Fajaryanto, I. A. Zulkarnain, F. Masykur, and Y. Litanianda, "Implementasi Internet Aman Di Fasilitas Umum Desa Ngrupit Kabupaten Ponorogo Menggunakan Web Proxy," *Jurnal Pengabdian Kepada Masyarakat Bersinergi Inovatif*, vol. 2, no. 1, pp. 206-214, 2024.
- [4] S. Bahri and D. E. R. Purba, "Implementasi Web Proxy pada Mikrotik untuk Menciptakan Internet Sehat pada SMK Al Maksum Langkat," *Jurnal Teknik Informatika Unika St. Thomas (JTIUST)*, vol. 7, no. 2, Dec. 2022.
- [5] R. Yakub, M. Tahir, E. P. Dewi, B. H. Khotimah, A. N. Afidha, and M. Y. Bahytsany, "Implementasi Keamanan Jaringan Wireless Menggunakan Web Proxy pada Mikrotik di SMP Negeri 1 Labang," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 4, Aug. 2025.
- [6] R. F. Anwar and H. Setiawan, "Implementasi Mikrotik RB941-2ND-TC sebagai Pemblokiran Situs dengan Menggunakan Web Proxy," *Artikel Inovatif*, Universitas Jenderal Achmad Yani, Dec. 18, 2024.
- [7] K. Angeria and A. R. W. Mahfuzhi, "Pembatasan Hak Akses dengan Menggunakan Web Proxy Berbasis Mikrotik," *Jurnal JUPITER*, vol. 17, no. 1, pp. 111-118, Jan. 2025.
- [8] K. Aziz, S. Zakir, W. Aprison, and L. Efriyanti, "Implementasi Keamanan Jaringan dengan Metode Firewall Filtering Menggunakan Mikrotik di SMKN 3 Payakumbuh," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 3, Jun. 2024.
- [9] A. U. Wuhi, F. Hariadi, and N. B. Uly, "Implementasi Web Filtering Firewall untuk Mendukung Internet Sehat di SMP Negeri 4 Mauliru," *JTIF | Jurnal Inovatif Wira Wacana*, vol. 3, no. 1, pp. 43-53, Apr. 2024.
- [10] Yuisar, L. Yulianti, and Y. S. H. Suzantry, "Analisa Pemanfaatan Proxy Server sebagai Media Filtering dan Caching pada Jaringan Komputer," *Jurnal Media Infotama*, vol. 11, no. 1, Feb. 2015.
- [11] F. Septian, M. H. Arfian, J. S. Asri, dan B. Tjahjono, "Pengujian Keamanan Website dengan Metode Penetration Testing (Studi Kasus: Universitas Esa Unggul)," *Innovative: Journal Of Social Science Research*, vol. 4, no. 5, hlm. 3629-3647, 2024.
- [12] 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)*, Universitas Muhammadiyah Tangerang, vol. -, no. -, pp. 298-306, Oct. 2021.
- [13] Yunanri W., Y. B. Fitriana, A. Susanto, E. S. Susanto, F. Hamdani, M. Rizky, dan N. Oper, "Implementasi Filtering Alamat Website Pada Web Proxy Menggunakan Raspberry-Pi," *Jurnal Informatika: Jurnal Pengembangan IT (JPIT)*, vol. 7, no. 1, hlm. 55-60, Jan. 2022.
- [14] A. S. Ma'mun and G. Z. Muflih, "Implementasi Web Filtering Firewall untuk Keamanan pada Jaringan Internet di Pondok Pesantren Al Hidayah Kebumen," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 8, no. 1, pp. 46-59, Jan. 2025.
- [15] R. Maulana, M. Hatta, dan I. Syafrinal, "Analisa Penerapan Filtering Proxy Server pada Keamanan Jaringan Komputer untuk Meminimalisir Penyebaran Malware (Studi Kasus Cakrabuana Cruiseship & School Cirebon)," *Jurnal Digit*, vol. 12, no. 1, hlm. 64-73, Sep. 2021.