P-ISSN: | E-ISSN:
Vol. 2, No. 1, Februari 2026, p.19-25

Journal of SONIC

Research Article [OPEN ACCESS]

Desain Topologi dan Implementasi *Firewall* IPFire dengan *URL Filtering* untuk Mitigasi Akses Situs Judi Online

Karno Ganjar Prasetyo[1]
D4 Teknologi Rekayasa Perangkat Lunak, Politeknik Bisnis Digital Indonesia
Email: karnogp@polbis.ac.id

ABSTRAK

Di Indonesia, perjudian online menjadi permasalahan besar di masyarakat. Metode pemblokiran konvensional, seperti *Filter DNS*, seringkali tidak efektif untuk domain baru. Tujuan dari penelitian ini adalah untuk menerapkan *Firewall IPFire* dengan pemblokiran *URL* berbasis kata kunci untuk meminimalkan akses ke situs judi online. Metode yang digunakan adalah *Network Development Life Cycle* (NDLC), yang mencakup simulasi implementasi dan desain topologi jaringan *virtual*. Untuk mencegah pencarian kata kunci di mesin pencari yang mengandung istilah judi slot dan judi online, melalui *content filtering IPFire*. Hasilnya menunjukkan bahwa metode pemblokiran kata kunci terbukti sangat efektif dalam mencegah akses ke konten judi di internet sejak tahap pencarian, metode tersebut lebih unggul dibandingkan dengan metode pemblokiran domain secara manual. Ini adalah solusi *Firewall IPFire* yang responsif dan berbiaya rendah untuk keamanan akses konten digital.

Kata kunci: *IPFire, Firewall, URL Filter, Judi Online, Judi Slot*

1. PENDAHULUAN

Pesatnya perkembangan teknologi dan internet telah memberikan dampak signifikan dalam berbagai aspek kehidupan, termasuk kemudahan akses informasi dan hiburan. Akan tetapi, kemajuan tersebut juga membawa masalah serius, salah satunya adalah maraknya akses ke situs-situs yang bersifat ilegal atau merugikan, khususnya perjudian online. Perkembangan teknologi informasi ikut member konstribusi bisnis perjudian semakin berkembang. Judi senantiasa membawa akibat buruk bagi masyarakat. Oleh kerena itu, sikap masyarakat pada dasarnya sangat setuju diberantasnya judi secara berlanjut, tegas tanpa pandang bulu terhadap para pelaku sehingga timbul tampak jera dan sadar bahwa judi adalah penyakit Masyarakat(Tasya Jadidah dkk., 2023).

Indonesia saat ini menduduki peringkat pertama negara dengan jumlah pemain judi slot online terbanyak di Asia Tenggara. Data ini menunjukkan betapa seriusnya permasalahan perjudian online di Indonesia. Dimana judi *online* tidak hanya menyebabkan kerugian finansial yang besar, tetapi juga dapat menimbulkan dampak negatif lain seperti masalah sosial dan kesehatan mental (Wahidaturrahmi & Priyanto, t.t.). Situasi tersebut menunjukkan adanya kebutuhan mendesak untuk mekanisme pengamanan jaringan yang efektif dan efisien untuk membatasi akses masyarakat dari konten berbahaya dan kejahatan siber lainnya, seperti judi online, penipuan online, dan konten ilegal.

Pemerintah serta penyedia layanan internet telah berusaha memblokir akses ke alamat situs slot judi *online*. Salah satu cara yang sering digunakan adalah *DNS Filtering*, yang berfokus pada pemblokiran berdasarkan nama domain situs (Magnusson, 2024). Meskipun pendekatan ini cukup ampuh, pemblokiran daftar domain yang terlarang masih dilakukan dengan cara manual atau semi-otomatis, sehingga membuatnya sulit dan memakan waktu mengingat banyaknya domain baru yang terus muncul. Masalah ini mengharuskan perlunya solusi keamanan jaringan yang lebih cepat dan terautomasi agar dapat meningkatkan efisiensi dan konsistensi dalam sistem pemblokiran.

Penelitian ini berfokus pada pemblokiran situs berbasis kata kunci, seperti "judi slot" atau "judi online". Hasil penelitian ini diharapkan dapat memberikan kontribusi praktis berupa model responsif dan

murah untuk mengamankan konten digital. Ini akan sangat relevan untuk diadopsi oleh masyarakat luas atau jaringan institusi.

2. METODE (EXPERIMENTAL) / LITERATURE REVIEW, HYPOTHESES, AND METHODS (ANALYSIS) / LITERATURE REVIEW AND METHODS (SLR)

Salah satu mekanisme pertahanan jaringan yang fundamental adalah *firewall* (Adhi Purwaningrum dkk., t.t.), dan metode pemblokiran yang umum digunakan oleh penyedia layanan adalah DNS Filtering. Penelitian sebelumnya telah menunjukkan bahwa DNS *Filtering* mampu memblokir domain berdasarkan basis data domain yang dilarang. Dalam upaya meningkatkan efisiensi, studi terdahulu telah mengimplementasikan otomatisasi pembaruan daftar blokir melalui CI/CD *pipeline* pada router Mikrotik untuk mengurangi waktu konfigurasi dan meningkatkan konsistensi pemblokiran domain (Wahidaturrahmi & Priyanto, t.t.).

Sedangkan pada penelitian lainnya dari Imam Riadi (*Filter berbasis mikrotik*, t.t.) mengenai keamanan jaringan yang berfokus pada perangkat router yang populer, seperti Mikrotik, dengan mengandalkan mekanisme DNS *Filtering* atau *Firewall Filter*. Efektivitasnya sangat bergantung pada kelengkapan daftar domain. Jika situs judi berganti domain atau menggunakan domain baru yang belum terdaftar, pemblokiran akan gagal. Bahkan beban kerja router mikrotik menjadi lebih berat, yaitu sebagai router dan sebagai *filtering* domain. Di sisi lain (Ramadhan & Fauzan, 2023) menerapkan pemblokiran kata kunci dan domain berbasis ekstensi web pada mesin peramban Google Chrome melalui Chrome Webstore.

Metode yang digunakan dalam penelitian ini adalah *Network Development Life Cycle* (NDLC). NDLC adalah pendekatan berstruktur untuk pengembangan jaringan yang melibatkan serangkaian langkah terorganisir, mulai dari perencanaan hingga implementasi (Aryanti & Aspriyono, t.t.). Penelitian ini melalui enam tahapan utama:

1. Tahap Analisis: Melakukan studi literatur untuk mengumpulkan informasi tentang keamanan firewall, URL filtering, dan mengidentifikasi daftar kata kunci terkait judi *online* dan judi slot.
2. Tahap Desain: Melakukan perancangan topologi jaringan virtual dan perancangan skenario pengujian.
3. Tahap Simulasi *Prototyping*: Melakukan simulasi percobaan pada mesin virtual untuk implementasi dan pengujian sistem.
4. Implementasi: Menerapkan rancangan yang telah disetujui ke dalam sistem yang sebenarnya, termasuk instalasi perangkat keras dan konfigurasi perangkat lunak.
5. Monitoring: Memantau kinerja jaringan secara berkelanjutan untuk memastikan jaringan berfungsi sesuai harapan.
6. Manajemen: Mengelola dan memelihara jaringan secara keseluruhan setelah implementasi untuk menjaga stabilitas dan efisiensinya.

Network Interface IPFire mengacu pada empat jenis antarmuka (*RED, GREEN, BLUE, ORANGE*) yang digunakan untuk membedakan segmen jaringan. *RED* adalah antarmuka ke internet, *GREEN* ke jaringan lokal (LAN), *BLUE* opsional untuk jaringan nirkabel atau terpisah, dan *ORANGE* opsional untuk server yang dapat diakses publik (Jakobsson dkk., t.t.).

IPFire terdiri dari 4 (empat) *Network Interface Red, Green, Blue* dan *Orange* (Jakobsson dkk., t.t.).

1. *Red Network Interface*, koneksi ini digunakan untuk koneksi dari IPFire ke Modem atau Router.
2. *Green Network Interface*, koneksi ini digunakan untuk koneksi dari IPFire ke Jaringan komputer client yang melalui Switch.
3. *Blue Network Interface*, koneksi ini merupakan pilihan, koneksi ini digunakan untuk koneksi dari IPFire ke Wireless
4. *Orange Network Interface*, koneksi ini merupakan pilihan, koneksi ini digunakan untuk *Demilitarized Zone* (DMZ) untuk operasional server, seperti Web Server dan Email Server.

2.1 Bahan dan Instrumen Penelitian

Penelitian ini menggunakan pendekatan eksperimental melalui simulasi yang dilakukan di lingkungan jaringan *virtual*. Sebelumnya (Yuliansyah, 2018) telah menerapkan internet sehat dengan menggunakan simulasi virtual machine. Bahan dan instrumen yang digunakan dirancang untuk mereplikasi kondisi jaringan berskala kecil hingga menengah di mana *Firewall* IPFire berfungsi sebagai *gateway* utama, sesuai dengan tahapan *Network Development Life Cycle* (NDLC).

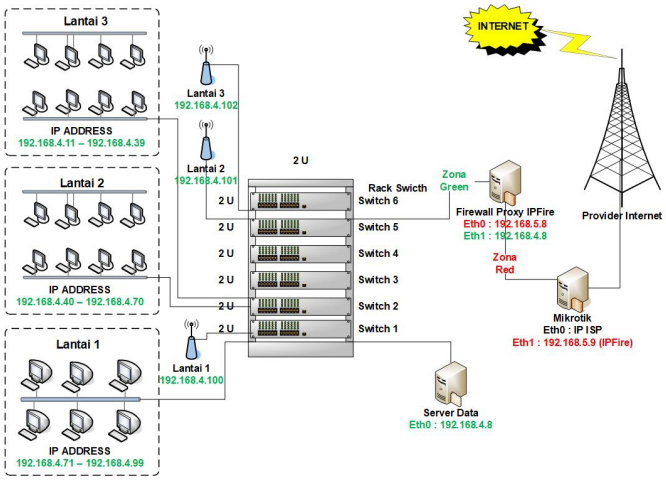
Simulasi jaringan dibangun menggunakan *platform* virtualisasi untuk memastikan isolasi dari jaringan produksi dan memungkinkan pengujian yang terkontrol serta dapat direplikasi.

Table 1. Spesifikasi dan Perangkat Lunak Uji Coba

Kategori	Instrumen/Data	Spesifikasi Teknis	Fungsi dalam Penelitian
Perangkat Keras Host	Komputer *Workstation*	Spesifikasi *hardware* minimum untuk menjalankan virtualisasi (CPU 4 Core, RAM 8GB)	Host utama untuk menjalankan lingkungan virtualisasi secara keseluruhan.
Platform *Virtualisasi*	VMware *Workstation* Pro	Versi 16 atau lebih tinggi	Digunakan sebagai *hypervisor* untuk mengalokasikan sumber daya dan menjalankan mesin *virtual*.
Sistem Utama (*Firewall*)	IPFire	Distribusi Linux khusus Firewall (Versi stabil terbaru saat penelitian)	Berfungsi sebagai gateway utama, firewall stateful inspection, dan implementasi Content Filter (Proxy Squid/SquidGuard).
Klien Pengujian	Mesin *Virtual* Klien	Sistem Operasi Windows 10/Linux Desktop	Digunakan untuk melakukan browsing, simulasi pencarian kata kunci judi online, dan pengujian akses.

2.2 Desain Topologi Jaringan

Topologi *star extended* merupakan perancangan bentuk topologi yang akan digunakan pada penelitian ini. Rangkaian dalam pengembangan jaringan komputer LAN sesuai dengan kebutuhan dari tiap komputer client terdapat pada tiap alur jaringan yang nantinya diterapkan (Sulistyo, 2022). Topologi *star extended* adalah gabungan beberapa topologi star standar yang dihubungkan menjadi satu hierarki. Ini memungkinkan jaringan yang lebih besar dengan menghubungkan beberapa hub atau switch ke switch utama yang menghubungkan semua bagian jaringan. Topologi ini sangat berguna untuk jaringan di sekolah atau universitas karena dapat menampung banyak perangkat (Entin Monika & Fitriah Fitriah, 2025).



Gambar 1. Desain Topologi

Topologi ini mengadopsi model *Red* dan *Greeen* pada IPFire, yang meliputi:

1. Zona *RED*: Antarmuka yang terhubung ke Internet.
2. Zona *GREEN*: Jaringan lokal aman (LAN) dengan skema alamat IP statis dan DHCP.
3. Klien Uji: Sebuah mesin virtual (OS Windows/Linux) yang terhubung ke Zona *GREEN*, digunakan untuk menguji akses *browsing*.

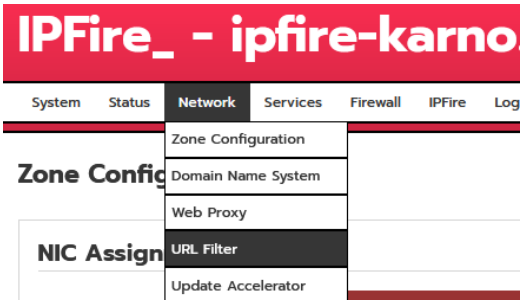
2.3 Prosedur Implementasi dan Pengujian

Implementasi URL Filtering dilakukan melalui *Content Filter* yang terintegrasi di IPFire. Sebanyak 10 kata kunci spesifik terkait judi online dan judi slot (misalnya: slot gacor, deposit pulsa, judi bola, dll.) dimasukkan ke dalam daftar *Custom expression list* pada *Content Filter*.

Gambar 2. Proses Instalasi IPFire

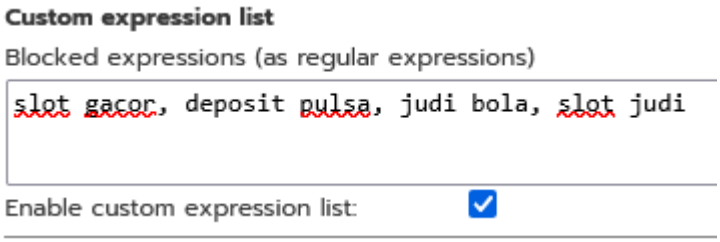
Gambar 3. Network Configuration

Sesuai dengan topolgi yang telah dibuat, Pada pilihan *Network Interface* yang dipilih yaitu Green dan Red, pada topologi koneksi *wireless* terhubung pada *Network Interface* Green.



Gambar 4. Fitur URL Filter

Filter URL di IPFire adalah fitur yang menggunakan proxy web untuk memblokir akses ke situs web berdasarkan kategorinya, seperti pada Gambar 4. Fitur ini diaktifkan dan dikonfigurasi di bagian Pengaturan Proxy Web dan memungkinkan pembuatan daftar blokir kustom seperti kata kunci tertentu untuk membatasi konten tidak pantas atau berbahaya, seperti pada Gambar 5.



Gambar 5. Kata kunci yang di blokir di URL Filter

3. HASIL DAN PEMBAHASAN

Bagian Hasil ini menyajikan temuan empiris dari implementasi *Firewall* IPFire yang dilakukan dalam lingkungan simulasi jaringan virtual, sesuai dengan tahapan *Network Development Life Cycle* (NDLC). Penelitian berfokus pada efektivitas *Content Filtering* berbasis kata kunci.

Topologi jaringan diimplementasikan dengan IPFire berfungsi sebagai gateway dan titik kontrol keamanan utama. Topologi ini memanfaatkan arsitektur zona warna IPFire, memisahkan Zona RED (Jaringan Luar/Simulasi Internet) dari Zona GREEN (Jaringan Lokal Aman). Semua klien uji di Zona GREEN diwajibkan melewati Proxy Transparan IPFire untuk memastikan seluruh lalu lintas web diperiksa oleh Content Filter.

Pengujian fungsionalitas dilakukan dengan menggunakan 10 kata kunci spesifik terkait judi online dan judi slot yang dimasukkan ke dalam daftar *Custom expression list* pada Content Filter IPFire.

Table 2. Ringkasan Hasil Uji Fungsionalitas Pemblokiran

Skenario Uji	Deskripsi Aksi	Hasil yang Diharapkan	Hasil Pengujian	Status Fungsionalita
Pencarian (Skenario Utama)	Mencari kata kunci (judi slot, slot gacor) di Google/Bing.	Akses ke query string diblokir, Error Page ditampilkan	Content Filter mendeteksi kata kunci di URL dan menampilkan halaman *Access Denied*.	100% Berhasil
Akses URL Langsung	Mengakses domain yang URL-nya mengandung kata kunci.	Akses ditolak oleh *Content Filter*.	Akses ditolak, ditampilkan halaman *Forbidden*.	100% Berhasil
Kata Kunci Tersamar	Mencari kata kunci tanpa spasi (judislotonline).	Pemblokiran tetap terjadi	Pemblokiran berhasil, menunjukkan kemampuan *Custom expression list* yang baik.	100% Berhasil

Hasil menunjukkan bahwa IPFire mampu melakukan pencegahan *pre-emptive* (pencegahan dini) dengan keberhasilan 100%. Ketika komputer klien melakukan pencarian, Content Filter mendeteksi keberadaan kata kunci dalam *query string* URL dan menampilkan pemblokiran sebelum klien menerima hasil pencarian dari search engine. Hal ini diverifikasi melalui *Log* IPFire yang mencatat *denied request* dari proxy IPFire.

4. KESIMPULAN

Tujuan utama penelitian ini adalah mengimplementasikan *Firewall* IPFire dengan URL *Filtering* berbasis kata kunci untuk mitigasi akses situs judi *online*, mengatasi inefektivitas DNS Filtering konvensional terhadap domain baru. Hasil pengujian menunjukkan bahwa metode pemblokiran kata kunci terbukti 100% efektif dalam mencegah pengguna mengakses konten judi sejak tahap pencarian, memvalidasi hipotesis penelitian. Keberhasilan ini dicapai melalui deteksi query string di URL *Filter* IPFire. Secara operasional, solusi ini lebih unggul dan efisien dari segi pemeliharaan dibandingkan metode pemblokiran domain manual atau terotomasi, karena tidak bergantung pada pembaruan daftar domain yang masif dan berkelanjutan, menjadikannya solusi *low-cost* yang responsif.

Implikasi dari temuan ini sangat signifikan bagi praktik keamanan jaringan, menawarkan model pertahanan yang agile untuk lingkungan berskala kecil. Meskipun metode ini memiliki keterbatasan terkait lalu lintas yang sepenuhnya terenkripsi (HTTPS/DoH), kontribusi utamanya adalah penyediaan kerangka kerja yang memprioritaskan pencegahan dini berbasis konten alih-alih pemblokiran berbasis alamat. Untuk penelitian di masa depan, disarankan untuk menguji SSL *Interception* pada IPFire dan mengintegrasikan model kecerdasan buatan (AI) guna mengotomatisasi pembaruan daftar kata kunci dan memperkuat pertahanan terhadap celah keamanan yang ada.

5. REFERENSI

Adhi Purwaningrum, F., Purwanto, A., Agus Darmadi, E., Tri Mitra Karya Mandiri Blok Semper Jomin Baru, P., & -Karawang, C. (t.t.). *OPTIMALISASI JARINGAN MENGGUNAKAN FIREWALL*.

Aryanti, S., & Aspriyono, H. (t.t.). PENGEMBANGAN SISTEM KEAMANAN JARINGAN WIFI BERBASIS MIKROTIK MENGGUNAKAN METODE NETWORK DEVELOPMENT LIFE CYCLE (NDLC). *Desember Jurnal TEKNOSIA*, *17*(2), 88–95. https://ejournal.unib.ac.id/index.php/teknosia

Entin Monika, & Fitriah Fitriah. (2025). PERANCANGAN JARINGAN LOCAL AREA NETWORK (LAN) DI SEKOLAH SMK 1 KEPAHIANG. *Jurnal Riset Sistem Informasi*, *2*(3), 126–133. https://doi.org/10.69714/r3dz5s66

Filter berbasis mikrotik. (t.t.).

Jakobsson, F., Ding, J., & Mellin, J. (t.t.). *Open source routing software*.

Magnusson, J. (2024). *Survey and Analysis of DNS Filtering Components*. http://arxiv.org/abs/2401.03864

Ramadhan, R. F., & Fauzan, A. (2023). Pembatasan Internet Berbasis Ekstensi Web pada Chrome Browser. *Proceedings Series on Physical & Formal Sciences*, *6*, 192–199. https://doi.org/10.30595/pspfs.v6i.869

Sulistyo, W. (2022). *Krea-TIF: Jurnal Teknik Informatika Model Keamanan Jaringan Menggunakan Firewall Port Blocking*. *10*(1), 10–18. https://doi.org/10.32832/kreatif.v10i1.6678

Tasya Jadidah, I., Milyarta Lestari, U., Alea Amanah Fatiha, K., Riyani, R., Ariesty Wulandari, C., Studi Pendidikan Guru Madrasah Ibtidaiyah, P., Islam Negeri Raden Fatah Palembang, U., & H Zainal Abidin Fikri, J. K. (2023). Analisis maraknya judi online di Masyarakat. Dalam *JISBI: Jurnal Ilmu Sosial dan Budaya Indonesia* (Vol. 1, Nomor 1).

Wahidaturrahmi, I., & Priyanto, D. (t.t.). *JUDI ONLINE BERBASIS DNS FILTERING*.

Yuliansyah, A. (2018). ANALISIS PENERAPAN MIKROTIK ROUTER SEBAGAI USER MANAGER UNTUK MENCIPTAKAN INTERNET SEHAT MENGGUNAKAN SIMULASI VIRTUAL MACHINE. *Technology Acceptance Model*, *9*(1), 62–66.