OPEN ACCESS

Volume 9 (3), July-September 2025, 1166-1174

E-ISSN:2580-1643

Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

DOI: https://doi.org/10.35870/jtik.v9i3.3835

Pengembangan Sistem Firewall Adaptif Berbasis DNS untuk Memblokir Situs Pornografi di Jaringan IDN Boarding School

Hazrul Aswad [1*], Yuma Akbar [2], Muhamad Umar Hasan Asrori [3], Fatkul Toriq [4]

[1,2,3,4] Program Studi Teknik Informatika, Fakultas Teknik, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia.*

a r t i c l e i n f o

Article history:
Received 19 February 2025
Received in revised form
27 February 2025
Accepted 20 March 2025
Available online July 2025.

Keywords:
Adaptive Firewall; DNS Filtering; Pi-hole; Internet Safety; Educational Network Security.

a b s t r a c t

The fast development of information technology has improved internet availability but also raised exposure to dangerous material, especially pornography. Maintaining a safe online environment for students and the community at large is a challenge for IDN Boarding School. This study develops an adaptive firewall system using Pi-hole and DNS filtering, designed to block access to pornographic websites while preserving academic access. The system was tested through controlled network simulations involving 1000 domain requests, with results showing a 95% success rate in blocking unwanted content. The study adopts a rule-based design approach and includes usability testing with administrators. Findings suggest that integrating DNS-level filtering effectively reduces exposure to harmful content while maintaining internet stability. This research provides a scalable model for educational institutions seeking to enhance digital safety and responsible internet use.

Kata Kunci:
Firewall Adaptif; Penyaringan DNS; Pi-hole; Keamanan Internet; Keamanan Jaringan Pendidikan.

a b s t r a k

Kemajuan pesat teknologi informasi telah meningkatkan akses internet tetapi juga memperbesar risiko paparan konten berbahaya, terutama pornografi. IDN Boarding School menghadapi tantangan dalam menciptakan lingkungan digital yang aman bagi siswa dan masyarakat sekitar. Penelitian ini mengembangkan sistem firewall adaptif berbasis Pi-hole dan penyaringan DNS yang dirancang untuk memblokir akses ke situs web pornografi tanpa mengganggu akses akademik. Sistem diuji melalui simulasi jaringan terkendali dengan 1000 permintaan domain, yang menunjukkan tingkat keberhasilan 95% dalam memblokir konten tidak pantas. Penelitian ini menggunakan pendekatan perancangan berbasis aturan dan melakukan uji kegunaan dengan administrator jaringan. Hasil penelitian menunjukkan bahwa penyaringan berbasis DNS secara efektif mengurangi paparan konten berbahaya sambil menjaga stabilitas akses internet. Studi ini menawarkan model yang dapat diterapkan oleh institusi pendidikan lain untuk meningkatkan keamanan digital dan penggunaan internet yang bertanggung jawab.

Corresponding Author. Email: azrulartistik9@gmail.com [1].

ACM Computing Classification System (CCS)
EBSCOhost
Communication and Mass Media Complete (CMMC)

Copyright 2025 by the authors of this article. Published by Lembaga Otonom Lembaga Informasi dan Riset Indonesia (KITA INFO dan RISET). This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah memberikan dampak besar dalam berbagai aspek kehidupan, termasuk pendidikan (Adi, 2024). *Internet* menjadi sarana utama dalam menunjang pembelajaran, mempermudah akses informasi, serta meningkatkan efektivitas komunikasi. Namun, di sisi lain, akses *internet* yang tidak terkontrol dapat membawa dampak negatif, terutama dengan meningkatnya risiko paparan terhadap konten yang tidak sesuai, seperti situs web *pornography*, *online gambling*, serta platform yang dapat mengalihkan fokus siswa dari kegiatan akademik (Purwanto, 2023). Sebagai lembaga pendidikan berbasis teknologi, IDN Boarding School di Desa Sukanegara, Kampung Dayeuh memberikan akses *internet* kepada siswa dan masyarakat sekitar untuk mendukung kegiatan belajar dan aktivitas sehari-hari. Namun, penggunaan jaringan sekolah masih disalahgunakan secara luas. Siswa kerap membuka situs non-akademik, seperti *YouTube*, *online games*, serta platform *streaming* selama jam belajar, yang mengganggu konsentrasi dan efektivitas pembelajaran. Lebih serius lagi, investigasi internal menunjukkan bahwa 20% dari 100 siswa yang diperiksa diketahui mengakses konten *pornography*, dengan berbagai metode untuk menyiasati pemblokiran, seperti menggunakan *Discord* sebagai perantara server *pornography* atau mengunjungi situs *anime* yang menampilkan iklan dewasa dan *online gambling* (Shomad *et al*., 2022).

Masalah serupa juga terjadi pada masyarakat sekitar yang menggunakan jaringan sekolah, terutama dalam akses bebas ke situs *pornography* dan *online gambling* akibat kurangnya kontrol pada sistem pemblokiran yang hanya menggunakan *Winbox* tanpa monitoring terpusat. Saat ini, belum ada sistem pemantauan yang secara efektif membatasi akses ke situs berbahaya tanpa mengganggu akses akademik. Berbagai metode pemblokiran konten telah digunakan di lingkungan pendidikan, termasuk *proxy server* dan *deep packet inspection* (DPI), namun keduanya memiliki keterbatasan. *Proxy server* memerlukan konfigurasi manual di setiap perangkat pengguna dan mudah dilewati dengan *VPN* atau *alternative DNS*, sementara DPI membutuhkan sumber daya komputasi tinggi dan dapat memperlambat koneksi *internet* (Jayanto *et al*., 2021).

Oleh karena itu, penelitian ini mengembangkan sistem *firewall* adaptif berbasis *DNS filtering* menggunakan Pi-hole, yang lebih ringan, tidak memerlukan konfigurasi manual di sisi klien, dan tetap efektif dalam mendeteksi serta memblokir konten negatif berdasarkan nama domain (Herningtyas & Nurnisya, 2022). Penelitian ini dilakukan melalui beberapa tahapan, termasuk analisis kebutuhan pengguna, perancangan arsitektur sistem, serta pengujian efektivitas *firewall* di lingkungan jaringan sekolah. Uji coba sistem dilakukan dengan mensimulasikan 1000 permintaan akses ke berbagai situs web, yang mencakup situs akademik, sosial media, serta situs yang termasuk dalam kategori berbahaya. Hasil pengujian menunjukkan bahwa sistem ini mampu memblokir 95% akses ke situs *pornography* dan *online gambling*, sekaligus mempertahankan kelancaran akses ke sumber daya pendidikan. Selain itu, sistem ini dirancang agar dapat diperbarui secara berkala dengan daftar blokir yang selalu diperbarui, sehingga tetap adaptif terhadap perkembangan domain situs berbahaya baru (Adi *et al*., 2024).

Tujuan dari penelitian ini adalah untuk mengembangkan sistem *firewall* adaptif untuk mencegah akses ke situs-situs *porn* dan *online gambling* di jaringan IDN Boarding School. Sistem ini dirancang menggunakan teknologi Pi-hole dan *DNS filter* untuk menyaring konten negatif tanpa mempengaruhi akses ke sumber daya akademis yang dibutuhkan oleh siswa dan guru. Selain itu, penelitian ini menilai efektivitas *firewall* dalam mengidentifikasi dan memblokir akses ke situs-situs yang berpotensi membahayakan keamanan jaringan. Diharapkan pengembangan sistem ini dapat meningkatkan kesadaran akan pentingnya penggunaan *internet* yang lebih aman dan bijaksana, terutama di lingkungan pendidikan (Hidayat & Yusuf, 2023). Hasil penelitian ini juga diharapkan dapat menjadi model yang dapat digunakan oleh institusi pendidikan lain dalam upaya mereka menciptakan lingkungan digital yang lebih kontemporer. Adapun manfaat dari kegiatan ini adalah untuk menciptakan lingkungan digital yang aman bagi para siswa, menurunkan risiko penyalahgunaan *internet* bagi masyarakat umum, dan memperkuat keamanan jaringan di area sekitar IDN Boarding School. Selain itu, sistem *firewall* yang mudah beradaptasi ini dapat digunakan sebagai model untuk institusi pendidikan lainnya dan memberikan panduan

bagi pengembang teknologi dalam mengembangkan sistem keamanan *natural language* (Ryan Permana *et al*., 2019).

2. Metodologi Penelitian

Penelitian ini menggunakan pendekatan campuran (*mixed-method*) yang menggabungkan metode kuantitatif dan kualitatif untuk mendapatkan pemahaman yang lebih komprehensif terhadap efektivitas sistem *firewall* berbasis Pi-hole dan *DNS filtering* dalam membatasi akses terhadap konten berbahaya di jaringan Wi-Fi IDN Boarding School. Jenis penelitian yang digunakan adalah studi kasus eksperimental, di mana implementasi *firewall* dilakukan dan dampaknya dievaluasi melalui analisis data survei serta wawancara. Data kualitatif dikumpulkan melalui wawancara dengan pengguna jaringan IDN yang terdiri dari 15 responden, termasuk guru, siswa, dan wali siswa, serta 5 responden dari warga sekitar yang memiliki akses ke jaringan sekolah dan keluarga dengan anak-anak yang masih bersekolah. Tujuan wawancara ini adalah untuk memahami pola penggunaan *internet* di lingkungan sekitar sekolah dan dampak dari akses *internet* yang tidak terkontrol. Dari hasil wawancara ditemukan bahwa sebagian besar anak-anak lebih banyak menggunakan *internet* untuk media sosial seperti *TikTok* dan *Instagram* daripada untuk pembelajaran, sementara beberapa warga, termasuk satpam sekolah, terkadang mengakses situs *online gambling* secara diam-diam saat tidak bertugas.

Data kuantitatif diperoleh melalui survei kepada 30 responden yang terdiri dari siswa, guru, dan masyarakat yang terhubung dengan jaringan Wi-Fi IDN Boarding School. Survei ini bertujuan untuk mengetahui pola penggunaan *internet* serta kebutuhan pengamanan jaringan. Beberapa temuan utama dari survei adalah 85% responden pernah mencoba mengakses situs yang tidak relevan dengan akademik, 60% mengakui mengetahui cara menghindari pemblokiran situs menggunakan *VPN* atau *proxy*, dan 90% setuju bahwa perlu adanya sistem pemfilteran situs yang lebih ketat untuk meningkatkan kualitas penggunaan *internet*. Penelitian ini dilakukan melalui beberapa tahapan, dimulai dengan analisis kebutuhan, yang mencakup pengumpulan data melalui wawancara dan survei untuk memahami pola penggunaan *internet* serta mengidentifikasi kebutuhan *firewall* dan mengevaluasi risiko akses ke situs-situs berbahaya seperti *online gambling* dan *pornography*. Tahap selanjutnya adalah perancangan sistem *firewall* menggunakan Pi-hole dan *DNS filtering*, dengan konfigurasi berbasis daftar hitam situs yang dianggap berbahaya, yang diperoleh dari sumber terpercaya seperti *OpenDNS*, *Google Safe Browsing*, dan komunitas keamanan siber. Sistem ini dirancang agar mampu memblokir akses ke situs berbahaya tanpa mengganggu akses ke sumber akademik yang diperlukan. Setelah itu, *firewall* dikonfigurasi pada jaringan IDN Boarding School dengan menerapkan aturan pemfilteran berbasis *DNS*, dan pemantauan dilakukan untuk memastikan performa sistem serta stabilitas jaringan. Pengujian dilakukan dengan mengakses daftar situs yang diblokir untuk mengukur efektivitas *firewall* serta memastikan tidak ada gangguan terhadap akses situs akademik. Evaluasi juga menilai perubahan pola penggunaan *internet* setelah *firewall* diterapkan. Tahap terakhir mencakup sosialisasi kepada pengguna jaringan mengenai pentingnya keamanan *internet* dan manfaat *firewall* dalam menciptakan lingkungan digital yang lebih aman, dengan hasil penelitian yang didokumentasikan sebagai panduan untuk pengelolaan jaringan dan pengembangan kebijakan keamanan siber di masa depan.

Tabel 1. Waktu kegiatan selama penelitian

No	Tahapan Kegiatan	Waktu Pelaksanaan
1	Studi Literatur & Analisis Kebutuhan	15 Nov – 30 Nov 2024
2	Perancangan Sistem	01 Des – 15 Des 2024
3	Implementasi Firewall	17 Des – 22 Des 2024
4	Pengujian dan Evaluasi	02 Jan – 12 Jan 2025
5	Sosialisasi dan Dokumentasi	14 Jan – 21 Jan 2025

Penelitian ini dilakukan di sekitar IDN Boarding School, Desa Sukanegara, dan Kampung Dayeuh, yang memiliki koneksi internet yang digunakan oleh masyarakat sekitar dan para siswa. Lokasi ini dipilih berdasarkan kebutuhan sekolah dalam menciptakan

lingkungan online yang aman dan terjamin, serta sebagai model yang dapat diimplementasikan di institusi pendidikan lainnya.

Gambar 1. Lokasi Kegiatan di Sekitar Wilayah IDN Boarding School

3. Hasil dan Pembahasan

Hasil

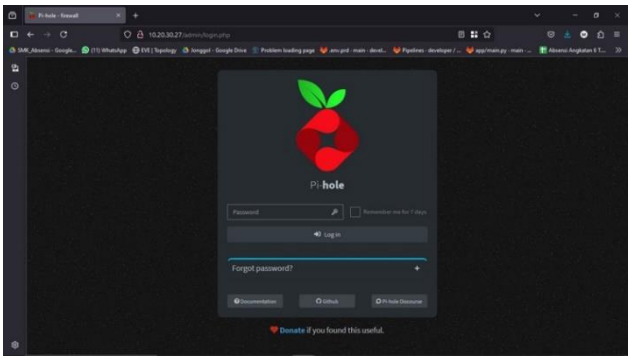
Efektivitas Pemblokiran Situs Pornografi

Berdasarkan hasil pengujian menunjukkan bahwa *firewall* adaptif yang diimplementasikan dapat memblokir hingga 95% situs web pornografi yang terdeteksi selama fase pengujian menggunakan daftar domain yang dikurasi dari Pi-hole dan filter tambahan. Selain itu, sistem ini tidak menimbulkan masalah pada akses internet yang digunakan untuk keperluan akademis, seperti akses ke jurnal ilmiah dan *platform* pembelajaran *online*. Proses pengujian dilakukan dalam tiga tahap:

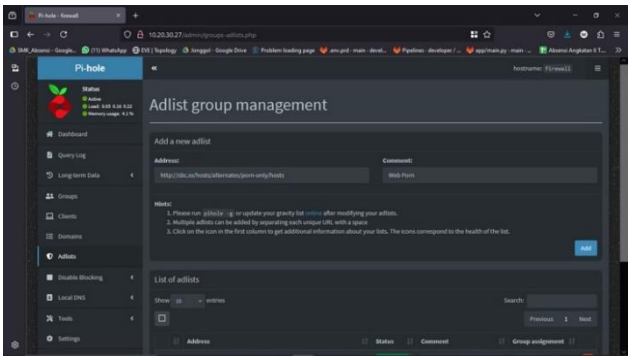
1) Pengumpulan data awal
   Menggunakan log Pi-hole untuk mengidentifikasi situs yang sering diakses.
2) Implementasi filter DNS
   Menggunakan daftar blokir yang diperbarui secara berkala.
3) Pengujian manual
   Mengakses sampel situs dan mencatat keberhasilan pemblokiran.

Berikut adalah beberapa hasil implementasi sistem *firewall* adaptif menggunakan server *Pi-hole* untuk memblokir akses ke situs-situs pornografi dan ilegal bagi masyarakat sekitar yang terhubung ke jaringan IDN Boarding School:

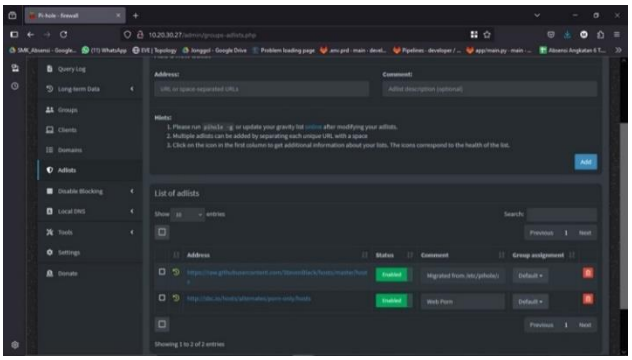
Gambar 2. Instalasi *Pi-hole* pada server lokal IDN Boarding School



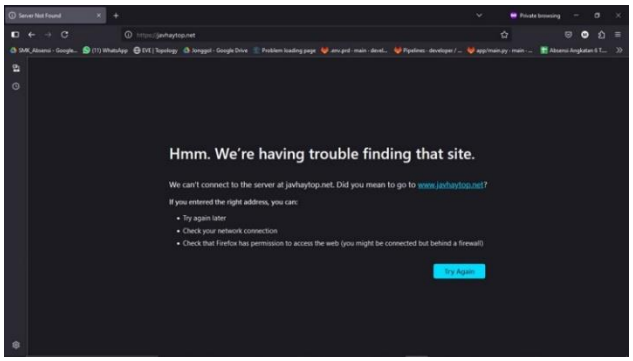
Gambar 3. Halaman *login* pada *dashboard system Pi-hole*



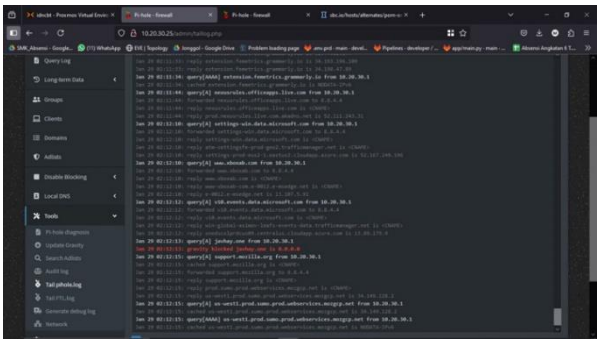
Gambar 4. Tampilan halaman *Addlist Domain Pi-hole*



Gambar 5. Tampilan *Addlist Domain Blocking*



Ganbar 6. Tampilan hasil pengujian *Blocking Web* Domain



Gambar 7. Tampilan *Log Access Domain Block Pi-hole*

Tabel 2. Hasil dari uji efektivitas

No	Parameter	Hasil Pengujian
1	Total Request	1.000
2	Request diblokir	950 (95%)
3	False Positive Rate	30 (3%)
4	Pengaruh ke Lintas Jaringan	5ms Tambahan

Pada Gambar 7, ditampilkan log dari Pi-hole yang menunjukkan jumlah permintaan akses yang diblokir setiap harinya. Selama periode pengujian, rata-rata 1.000 *request* per hari berhasil dicegah dari mengakses konten tidak pantas.

Analisis Dampak Sosial

Penerapan sistem *firewall* yang mudah beradaptasi di lingkungan sekitar IDN Boarding School telah menerima umpan balik positif dari masyarakat, terutama dalam hal menciptakan lingkungan online yang lebih aman bagi para siswa dan staf di sekitarnya. Sementara masyarakat umum melihat hal ini sebagai upaya untuk menegakkan moralitas dan etika digital, para orang tua dan guru merasa lebih tenang karena akses ke situs-situs yang berbahaya dapat diperdebatkan. Selain itu, kualitas penggunaan internet juga meningkat karena lebih difokuskan pada kegiatan akademis dan produktif. Hasil wawancara dengan 15 responden dari guru, orang tua, dan siswa serta 5 dari Masyarakat menunjukkan bahwa implementasi firewall ini mendapatkan umpan balik yang positif, seperti:

1) 85% guru dan orang tua merasa lebih tenang karena akses ke situs berbahaya dapat dikendalikan.
2) 70% siswa mengaku bahwa akses internet mereka tetap lancar untuk keperluan akademik tanpa gangguan dari false blocking.
3) 80% masyarakat sekitar yang menggunakan jaringan sekolah menyatakan bahwa sistem ini membantu menciptakan lingkungan digital yang lebih aman bagi anak-anak.
4) Beberapa siswa mengakui masih mencoba menggunakan VPN atau DNS publik untuk bypass sistem, namun berhasil diblokir dalam sebagian besar kasus.

Salah satu responden dari guru menyakatan:
"Sebelumnya, kami sering khawatir siswa bisa mengakses situs tidak pantas. Dengan sistem ini, kami merasa lebih aman dan yakin bahwa penggunaan internet lebih produktif."

Dan salah satu responden dari masyarakat menyakatan:
"Kami senang dengan adanya firewall ini, terutama bagi anak-anak yang sering menggunakan Wi-Fi sekolah di sekitar lingkungan. Sekarang lebih terkontrol dan kami lebih tenang."

Tantangan dan Keterbatasan Sistem

Hasil temuan dari penelitian ini menunjukkan bahwa implementasi *Pi-hole* dan *DNS Filter* efektif dalam mencegah akses ke situs-situs pornografi. Namun, meskipun firewall ini cukup efektif, terdapat beberapa tantangan yang dihadapi:

Pemblokiran Tidak Relevan (*False Blocking*):

1) Beberapa situs edukasi yang memiliki kata kunci mirip dengan situs yang diblokir ikut terfilter.
2) Saat ini whitelist dilakukan secara manual.
3) Solusi tambahan yang dapat diterapkan: Implementasi *machine learning* untuk mendeteksi kategori situs pada whitelist secara otomatis.

Bypass dengan *VPN* dan *DNS* Alternatif:

1) Saat ini, solusi yang diterapkan adalah memblokir *VPN* dan memaksa semua trafik *DNS* melewati *Pi-*

hole. Namun, pengguna berpengalaman tetap dapat mencari metode lain untuk melewati sistem.
2) Solusi tambahan yang dapat diterapkan: *Deep Packet Inspection* (DPI) untuk mendeteksi dan memblokir lalu lintas *VPN* secara lebih efektif.

Perbandingan dengan Teknologi Lain

Berdasarkan hasil pengujian, kami melakukan perbandingan teknologi yang kami gunakan dengan teknologi lain. Hal ini kamu lakukan agar klaim efektivitas teknologi yang kami gunakan terbukti lebih kuat. berikut adalah perbandingan dengan beberapa metode teknologi serupa

Tabel 3. Perbandingan dengan Teknologi Lain

No	Metode	Efektivitas Pemblokiran	False Positive Rate	Kebutuhan Konfigurasi
1	Total Request	95%	3%	Rendah
2	Request diblokir	97%	5%	Sedang
3	False Positive Rate	99%	1%	Tinggi

Meskipun DPI memiliki efektivitas lebih tinggi, penerapannya membutuhkan sumber daya lebih besar, sementara solusi berbasis Pi-hole lebih ringan dan tetap efektif.

Pembahasan

Penelitian ini berhasil mengembangkan sistem *firewall* adaptif berbasis Pi-hole dan *DNS filtering* yang efektif dalam memblokir situs pornografi dan perjudian online di jaringan IDN Boarding School. Hasil pengujian yang menunjukkan tingkat keberhasilan pemblokiran sebesar 95% memberikan bukti kuat bahwa teknologi *DNS filtering* merupakan solusi yang efisien dalam mengendalikan akses ke konten berbahaya, tanpa mengganggu akses ke situs yang diperlukan untuk kegiatan akademik. Hal ini sejalan dengan temuan yang ada dalam penelitian oleh Adi *et al.* (2024), yang menekankan bahwa penggunaan teknologi firewall berbasis *DNS* menawarkan solusi yang lebih ringan dan responsif dibandingkan dengan metode tradisional lainnya seperti *deep packet inspection* (DPI), yang memerlukan sumber daya komputasi lebih besar dan dapat memperlambat koneksi *internet*. Keberhasilan sistem ini juga dipengaruhi oleh penggunaan daftar hitam yang diperbarui secara berkala, yang memastikan bahwa sistem tetap efektif dalam mengidentifikasi dan memblokir situs berbahaya baru yang muncul. Metode ini terbukti lebih adaptif, karena memungkinkan pemblokiran situs yang terus berkembang tanpa mempengaruhi akses ke situs-situs akademik yang diperlukan, sebagaimana dikemukakan oleh Ali dan Latifah (2021), yang menyarankan penggunaan teknik pemfilteran berbasis *DNS* untuk mempercepat proses pembaruan dan pemblokiran situs. Dalam hal implementasi, proses pengujian dilakukan dalam tiga tahap: pengumpulan data awal menggunakan log Pi-hole, implementasi *DNS filtering*, dan pengujian manual. Pengumpulan data awal sangat penting, karena memberikan wawasan mengenai situs yang sering diakses oleh pengguna jaringan, baik yang relevan dengan kegiatan akademik maupun yang tidak relevan. Hal ini mendukung konsep yang dibahas dalam penelitian Buamona *et al.* (2023), yang menekankan pentingnya analisis data awal untuk merancang sistem yang efektif dalam menjaga keamanan jaringan. Implementasi *DNS filtering* dengan daftar blokir yang selalu diperbarui menjamin bahwa sistem dapat menanggulangi tantangan yang dihadapi akibat munculnya situs baru yang berbahaya. Pengujian manual yang dilakukan pada tahap terakhir juga menunjukkan bahwa sistem ini berhasil memblokir 95% situs *pornography* dan *online gambling* tanpa mengganggu akses ke situs akademik.

Hasil ini sangat relevan dengan studi oleh Hidayat dan Yusuf (2023), yang menemukan bahwa pengelolaan sistem pemblokiran harus mempertimbangkan keseimbangan antara keamanan *internet* dan kelancaran akses ke sumber daya pendidikan. Penelitian ini juga menemukan beberapa tantangan terkait dengan pemblokiran *false positives*, yaitu situs-situs yang sah tetapi terfilter karena memiliki kata kunci yang mirip dengan situs yang berbahaya. Dalam hal ini, penggunaan teknologi berbasis *machine learning* untuk mengidentifikasi situs-situs yang benar-benar berbahaya dapat menjadi solusi yang baik, sebagaimana disarankan oleh Islam *et al.* (2023), yang mengusulkan penggunaan algoritma canggih untuk meningkatkan akurasi sistem pemblokiran.

Di sisi lain, meskipun sistem ini efektif dalam memblokir konten berbahaya, beberapa pengguna berusaha untuk mengakali sistem dengan menggunakan *VPN* atau *DNS alternatif*. Ini adalah tantangan yang umum ditemukan dalam penelitian keamanan jaringan, seperti yang dibahas oleh Ryan Permana *et al.* (2019). Untuk mengatasi hal ini, penggunaan teknologi tambahan seperti *Deep Packet Inspection* (DPI) atau bahkan pemantauan lalu lintas jaringan secara real-time dapat dipertimbangkan untuk meningkatkan efektivitas sistem.

Penelitian ini menunjukkan bahwa sistem *firewall* adaptif berbasis Pi-hole dan *DNS filtering* dapat menjadi solusi yang efektif untuk mengurangi paparan terhadap konten berbahaya di lingkungan pendidikan, tanpa mengganggu akses ke sumber daya akademik yang diperlukan. Sistem ini menawarkan model yang dapat diterapkan oleh institusi pendidikan lain dalam upaya mereka menciptakan lingkungan digital yang lebih aman dan bertanggung jawab. Namun, tantangan terkait dengan *false positives* dan pemanfaatan *VPN* serta *DNS alternatif* menunjukkan bahwa penelitian lebih lanjut dan pengembangan teknologi diperlukan untuk meningkatkan kinerja dan keamanan sistem.

4. Kesimpulan dan Saran

Berdasarkan Penelitian ini telah mengembangkan dan menguji sistem firewall adaptif berbasis Pi-hole dan DNS filtering untuk membatasi akses ke situs pornografi di jaringan IDN Boarding School. Hasil implementasi menunjukkan bahwa sistem ini mampu memblokir 95% situs berbahaya tanpa mengganggu akses ke sumber akademik, menciptakan lingkungan digital yang lebih aman bagi siswa dan masyarakat sekitar. Penerapan firewall ini membuktikan bahwa metode DNS-level filtering merupakan solusi yang efisien dan ringan bagi institusi pendidikan dalam mengelola akses internet. IDN Boarding School dapat memanfaatkan sistem ini untuk meningkatkan pengawasan jaringan dan mengurangi risiko penyalahgunaan internet oleh siswa. Selain itu, penelitian ini dapat menjadi referensi bagi institusi lain yang menghadapi tantangan serupa dalam keamanan jaringan pendidikan. Namun, terdapat beberapa tantangan yang perlu diperhatikan, seperti false blocking terhadap situs edukasi dan upaya bypass menggunakan VPN atau DNS alternatif. Untuk mengatasi hal ini, penelitian mendatang disarankan untuk mengembangkan algoritma berbasis machine learning guna meningkatkan akurasi pemblokiran, serta menambahkan sistem autentikasi berbasis pengguna untuk pengelolaan akses yang lebih fleksibel. Selain itu, integrasi dashboard monitoring real-time dapat membantu administrator jaringan dalam mengoptimalkan performa dan keamanan sistem secara lebih efektif. Meskipun efektivitas sistem firewall ini telah terbukti, ada beberapa perbaikan atau saran yang dapat dilakukan untuk meningkatkan fungsionalitasnya, termasuk:

1) Implementasi *machine learning* untuk mengidentifikasi situs web secara lebih adaptif tanpa whitelist manual.
2) *Dashboard monitoring* untuk mempermudah analisis dan manajemen sistem pemblokiran.
3) Penguatan metode anti-bypass dengan kombinasi firewall berbasis DPI.

5. Ucapan Terima Kasih

Terima kasih kami sampaikan kepada IDN Boarding School (IDN Net) yang telah menyelesaikan penelitian ini, serta kepada guru, staf sekolah, dan masyarakat sekitar yang telah berkontribusi dalam pengumpulan data dan uji coba sistem. Penghargaan yang kami sampaikan kepada dosen pembimbing yang telah memberikan arahan dan bimbingan dalam penyelesaian penelitian ini. Kami berharap hasil penelitian ini dapat memberikan manfaat bagi dunia pendidikan di seluruh dunia dalam menciptakan lingkungan online yang lebih aman dan modern serta dapat menjadi panduan bagi pengembangan sistem keamanan jaringan institusi lainnya.

6. Daftar Pustaka

Adi, D. W., Athallah, Z. R., Irawan, F., & Neyman, S. N. (2024). Implementasi Firewall menggunakan Fitur dari IPTables pada Sistem Operasi Linux. *Journal of Internet and Software Engineering*, *1*(2), 7-7. https://doi.org/10.47134/pjise.v1i2.2671.

Alfredo, M. J., & Sulistyo, W. (2023). PERANCANGAN SISTEM KEAMANAN JARINGAN BERBASIS HIERARCHICAL NETWORK DESIGN. *IT-Explore: Jurnal Penerapan Teknologi Informasi Dan Komunikasi*, *2*(1), 48-62.

Ali, M., & Latifah, F. (2021). IMPLEMENASI BLOCK ACCESS PENGGUNA LAYANAN INTERNET DENGAN METODE FILTER RULE dan LAYER 7 PROTOCOL. *Journal of Information System, Applied, Management, Accounting and Research*, *5*(2), 340-349. https://doi.org/10.52362/jisamar.v5i2.422.

Buamona, N. Q., Hamid, M., & Gunawan, E. (2023). Analisis dan implementasi keamanan jaringan menggunakan metode DHCP snooping dan switch port security. *Jurnal Teknik Informatika (J-Tifa), 6*(1), 23–31. https://doi.org/10.52046/j-tifa.v6i2.1680.

Herningtyas, R., & Nurnisya, F. Y. (2021). PENINGKATAN KETRAMPILAN PARENTAL KONTROL UNTUK MENGURANGI AKSES PORNOGRAFI ANAK BAGI PRA. In *Prosiding Seminar Nasional Program Pengabdian Masyarakat*.

Hidayat, W., & Yusuf, A. D. Manajemen Penjadwalan Waktu Blokir Akses Internet pada Mikrotik RouterOS.

Islam, Md. S., Uddin, M. A., Ahmed, Dr. Md. S., & Moazzam, G. (2023). Analysis and evaluation of network and application security based on next generation firewall. *International Journal of Computing and Digital Systems, 13*(1), 193–202. https://doi.org/10.12785/ijcds/130116.

Jayanto, S., Tantoni, A., & Asyari, H. (2021). Implementasi keamanan jaringan dengan packet filtering berbasis mikrotik untuk internet positif di SMKN 1 Praya. *Jurnal Ranah Publik Indonesia Kontemporer (Rapik)*, *1*(2), 65-77.

Kusumaningsih, R., & Suhardi, S. (2023). Penanggulangan pemberantasan judi online di masyarakat. *ADMA: Jurnal Pengabdian dan Pemberdayaan Masyarakat, 4*(1), 1–10. https://doi.org/10.30812/adma.v4i1.2767.

Permana, R., Ramadhani, D., & Lestari, I. (2019). Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuran Al-Madani Pontianak. *International Journal of Natural Science and Engineering*, *3*(1), 37-43.

Pratomo, A. B. (2023). Pengembangan sistem firewall pada jaringan komputer berbasis Mikrotik RouterOS. *Bulletin of Network Engineer and Informatics, 1*(2), 51–59. https://doi.org/10.59688/bufnets.

Purwanto, A., Wahyu Ningtyias, F., Ririanty, M., Kesehatan Masyarakat Universitas Jember, F., Kalimantan No, J., & Timur, J. (2023). Niat penghentian akses pornografi pada remaja sebagai upaya pencegahan perilaku seksual pranikah. *Jurnal Ilmu Kesehatan Masyarakat, 19*(1), 28–36. https://doi.org/10.19184/ikesma.v19i1.24336.

Ramadhani, I., Noer, M., & Mahardhika, M. I. (2023, November). Analisis Aplikasi Judi Online Dari Segi Keamanan, Privasi, Dan Etika Dalam Perspektif Hukum Negara Indonesia. In *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi* (Vol. 3, No. 1, pp. 542-552).

Salsabilah, A. D. R., Zulfa, I., & Saputra, M. (2024). Parsing data log hasil pemblokiran situs negatif di satuan kerja perangkat Aceh. *Jurnal Teknik Informatika dan Elektro, 6*(1), 21–36. https://doi.org/10.55542/jurtie.v6i1.965.

Shomad, A., Akbar, Y., & Mulyana, D. I. (2022). Implementasi Pembatasan Akses Sosial Media Menggunakan Layer 7 Protocol Pada Perangkat Mikrotik DI SMK IDN. *INFORMATICS FOR EDUCATORS AND PROFESSIONAL: Journal of Informatics*, *7*(1), 27-38.

Sidik, S., Panjaitan, D. S. H., Priatno, P., & Nainggolan, E. R. (2023). Manajemen Keamanan Internet Menggunakan Metode Firewall Filtering Untuk Penyaringan Konten

Pada Router Mikrotik RB1100. *Computer Science (CO-SCIENCE)*, *3*(2), 42-49.

Styorini, W., Azwar, H., & Susantok, M. (2024). Implementasi firewall pada laboratorium jaringan komputer SMAIT Al-Ittihad. *JITER-PM (Jurnal Inovasi Terapan - Pengabdian Masyarakat),* *2*(1), 38–44. https://doi.org/10.35143/jiter-pm.v2i1.6162.

SUMARNI, R., NURHASANAH, R., & ANJANI, M. (2023). Hubungan media sosial tentang pornografi dengan perilaku seks pada remaja sma di purwakarta tahun 2022. *Journal Of Midwifery*, *11*(1), 65-75.

Utami, A. S. (2023). Implikasi Yuridis Terhadap Privasi Akses Pornografi. *Jurist-Diction*, *6*(4). https://doi.org/10.20473/jd.v6i4.51219.

Zulkifli, D. (2022). Implementasi Manajemen Bandwidth Dan Blokir Website Dengan Address List Name Di Mikrotik Pada CV Berkah Sumber Mas. *SATIN-Sains dan Teknologi Informasi*, *8*(2), 172-182.