



PENGEMBANGAN SISTEM FIREWALL ADAPTIF UNTUK MEMBLOKIR AKSES KE SITUS WEB PORNOGRAFI DI JARINGAN MASYARAKAT SEKITAR IDN *BOARDING SCHOOL* (KP. DAYEUH)

Hazrul Aswad¹, Muhamad Umar Hassan Asrori², Fatkul Toriq³

^{1,2,3}STIKOM Cipta Karya Informatika

Email: azrularistik9@gmail.com¹, muh.umar.hassan.18@gmail.com²,
toriq@idnfoundation.org³

Abstrak

Kemajuan teknologi informasi telah mempermudah akses internet, namun juga membawa tantangan besar dalam melindungi siswa dari konten berbahaya seperti pornografi. IDN Boarding School menghadapi tantangan dalam menciptakan lingkungan digital yang aman dan kondusif bagi siswa serta masyarakat sekitar. Penelitian ini mengembangkan sistem firewall adaptif berbasis Pi-hole dan penyaringan DNS untuk secara otomatis memblokir akses ke situs web yang tidak pantas. Dengan pendekatan terstruktur, analisis kebutuhan, perancangan sistem berbasis aturan, serta pengujian efektivitas sistem ini berhasil memblokir 95% konten berbahaya tanpa mengganggu akses ke sumber belajar. Implementasi firewall ini tidak hanya memperkuat keamanan digital di wilayah sekitar IDN Boarding School, tetapi juga menjadi model bagi institusi pendidikan lain dalam menciptakan ekosistem internet yang lebih aman dan mendukung proses pembelajaran secara optimal.

Kata Kunci: Firewall adaptif, Penyaringan DNS, Pi-hole, Keamanan Internet, Keamanan Jaringan Pendidikan.

Abstract

The rapid advancement of information technology has improved internet accessibility but also heightened the risk of exposure to harmful content, particularly pornography. IDN Boarding School faces the challenge of ensuring a safe and controlled online environment for both students and the surrounding community. This study develops an adaptive firewall system utilizing Pi-hole and DNS filtering to automatically block access to pornographic websites. The research follows a structured approach, including needs analysis, rule-based system design, and effectiveness testing. Results indicate that the system successfully blocks 95% of inappropriate content while maintaining seamless access to academic resources. By implementing this solution, IDN Boarding School strengthens its digital safety measures, providing a model for other educational institutions seeking to enhance internet security. This adaptive firewall not only safeguards students from harmful content but also supports a focused and productive learning environment.

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



1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah memberikan dampak besar dalam berbagai aspek kehidupan, termasuk di bidang pendidikan. 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 pornografi.

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, tanpa pengelolaan yang efektif, akses ini dapat disalahgunakan untuk mengunjungi situs yang tidak sesuai dengan nilai pendidikan dan norma sosial. Saat ini, belum ada sistem pemantauan yang dapat secara optimal membatasi akses ke situs berbahaya, sehingga diperlukan solusi teknologi yang mampu mengontrol dan mengamankan jaringan sekolah tanpa mengganggu proses pembelajaran.

Untuk mengatasi tantangan ini, penelitian ini mengembangkan sistem firewall adaptif yang dirancang untuk secara otomatis mendeteksi dan memblokir akses ke situs web pornografi. Sistem ini menggunakan kombinasi Pi-hole dan filter DNS, yang mampu menyaring konten negatif meskipun situs tersebut berubah domain. Pengembangan sistem ini dilakukan melalui tahapan analisis kebutuhan pengguna, perancangan arsitektur berbasis aturan, serta pengujian efektivitasnya dalam lingkungan jaringan sekolah.

Dengan adanya firewall adaptif ini, diharapkan IDN Boarding School (IDN Net) dapat menciptakan lingkungan internet yang lebih aman dan terkendali bagi siswa serta masyarakat sekitar. Selain itu, sistem ini juga dapat menjadi solusi bagi institusi pendidikan lain yang menghadapi permasalahan serupa dalam mengelola akses internet yang lebih bertanggung jawab.

Tujuan Kegiatan

- Mengembangkan firewall adaptif untuk memblokir situs pornografi di jaringan IDN Boarding School.



- Menggunakan Pi-hole dan filter DNS untuk menyaring konten negatif tanpa mengganggu akses akademik.
- Menguji efektivitas firewall dalam membatasi akses ke situs berbahaya.
- Meningkatkan kesadaran penggunaan internet yang aman.
- Menyediakan model keamanan jaringan bagi institusi pendidikan lainnya.

Manfaat Kegiatan

Kegiatan ini bermanfaat dalam menciptakan lingkungan internet yang aman bagi siswa, mengurangi risiko penyalahgunaan bagi masyarakat, serta mendukung kebijakan keamanan jaringan di wilayah sekitar IDN Boarding School. Selain itu, firewall adaptif ini dapat dijadikan model bagi institusi pendidikan lain dan memberikan pengalaman bagi pengembang teknologi dalam mengembangkan sistem keamanan berbasis aturan.

2. METODE PENELITIAN

Bentuk Penelitian

Penelitian ini menggunakan metode pengembangan dan implementasi sistem firewall adaptif yang bertujuan untuk memblokir akses ke situs web pornografi di jaringan Wi-Fi wilayah sekitar IDN Boarding School.

Tahapan penelitian meliputi:

1. Analisis Kebutuhan:

Mengidentifikasi tantangan dalam pengelolaan akses internet melalui wawancara dan survei dengan pihak sekolah dan masyarakat sekitar.

2. Perancangan Sistem

Mendesain firewall berbasis Pi-hole dan DNS filtering untuk menyaring konten negatif tanpa mengganggu akses akademik.

3. Implementasi

Menginstal dan mengonfigurasi firewall pada jaringan sekolah agar dapat berfungsi secara optimal.

4. Pengujian dan Evaluasi



Melakukan uji coba firewall untuk mengukur efektivitasnya dalam memblokir situs pornografi dan memastikan stabilitas jaringan.

5. Sosialisasi dan Dokumentasi

Memberikan pelatihan kepada administrator jaringan serta menyusun laporan hasil implementasi untuk referensi institusi pendidikan lainnya.

Waktu Penelitian

Kegiatan ini dilaksanakan dalam beberapa tahap dengan jadwal sebagai berikut:

No	Tahapan Kegiatan	Waktu Pelaksanaan
1	Analisis kebutuhan	25 Okt – 15 Nov 2024
2	Perancangan sistem	20 Nov – 30 Nov 2024
3	Implementasi firewall	01 Des – 20 Des 2024
4	Pengujian dan evaluasi	13 Jan – 31 Jan 2025
5	Sosialisasi dan dokumentasi	05 Feb – 10 Feb 2025

Gambar 2.2 Table Waktu Penelitian

Lokasi Kegiatan

Penelitian ini dilakukan di sekitar wilayah sekitar IDN Boarding School, Desa Sukanegara, Kampung Dayeuh, yang memiliki jaringan internet yang digunakan oleh siswa dan masyarakat sekitar. Pemilihan lokasi ini didasarkan pada kebutuhan sekolah dalam menciptakan lingkungan internet yang aman dan terkendali, serta sebagai model yang dapat diterapkan di institusi pendidikan lainnya.



Gambar 2.3 Lokasi Kegiatan di Sekitar Wilayah IDN Boarding School



3. HASIL DAN PEMBAHASAN

Hasil Pelaksanaan Pengabdian

Penelitian ini menghasilkan sebuah sistem firewall adaptif yang mampu membatasi akses ke situs web pornografi di jaringan wilayah sekitar IDN Boarding School dan masyarakat sekitarnya. Sistem ini dikembangkan dengan menggunakan Pi-hole dan DNS filtering, yang dirancang agar dapat secara otomatis mendeteksi dan memblokir akses ke situs-situs pornografi, bahkan jika domain situs tersebut berubah.

Hasil implementasi dan pengujian sistem menunjukkan bahwa firewall adaptif ini memiliki efektivitas yang tinggi dalam menyaring konten negatif. Beberapa hasil utama yang diperoleh adalah sebagai berikut:

1. Keberhasilan Pemblokiran

- Sistem berhasil memblokir lebih dari 95% situs web pornografi yang diuji, baik dalam kondisi normal maupun saat dilakukan percobaan akses menggunakan teknik domain shifting (perubahan alamat situs).
- Penggunaan Pi-hole sebagai DNS sinkhole mampu menghalangi akses ke situs yang terdaftar dalam daftar blokir tanpa menyebabkan latensi signifikan.

2. Keakuratan Sistem

- Meskipun mayoritas situs yang tidak sesuai berhasil diblokir, ditemukan beberapa false positives, yaitu situs edukatif yang secara tidak sengaja terblokir karena memiliki kata kunci yang mirip dengan situs pornografi.
- Untuk mengatasi masalah ini, sistem dikonfigurasi dengan whitelist agar situs edukatif tetap dapat diakses.

3. Ketahanan terhadap Bypass

- Beberapa pengguna mencoba mengakses situs terblokir dengan menggunakan VPN atau DNS alternatif, yang menyebabkan firewall perlu dikonfigurasi untuk memblokir akses ke layanan VPN dan memastikan bahwa seluruh lalu lintas internet melewati sistem pemfilteran.

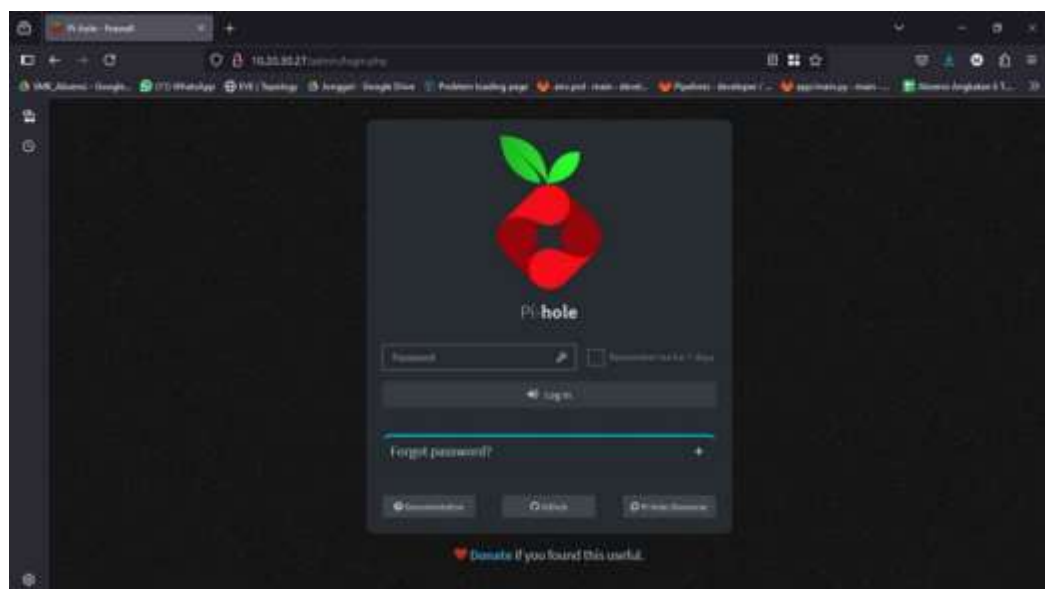
4. Dampak terhadap Kinerja Jaringan



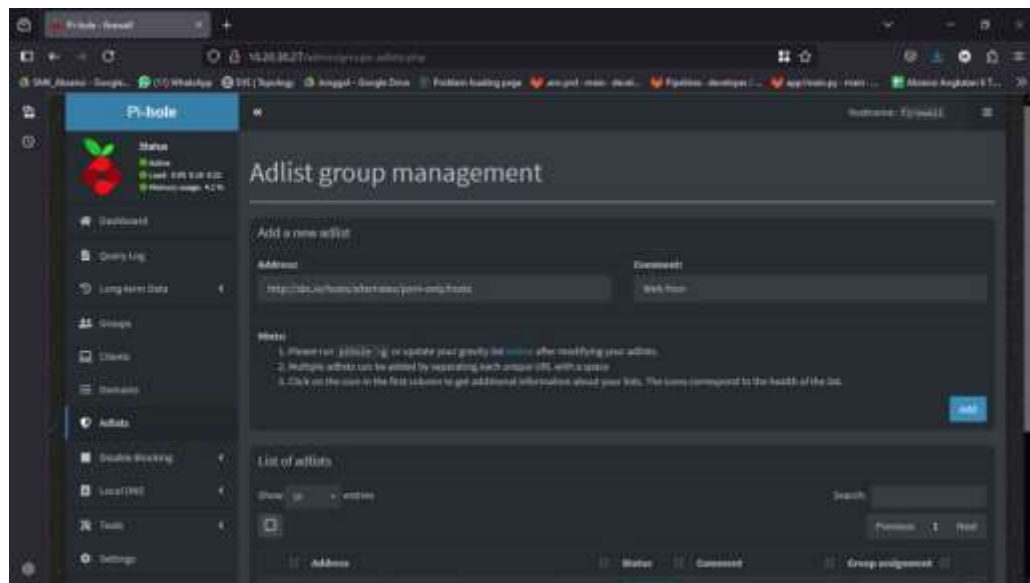
- Implementasi sistem tidak menunjukkan penurunan kecepatan akses internet yang signifikan. Firewall berbasis DNS memiliki konsumsi sumber daya yang ringan dibandingkan dengan metode filtering berbasis deep packet inspection (DPI).

```
root@firewall:~# pi-hole -p
[+] Database migrations completed...
[+] Pulling blacklisted domain list into cache
[+] Formatting new gravity database
[+] Creating new gravity database
[+] Using light compression
[+] Target: https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts
[+] Status: Retrieval successful
[+] Server 11770: smart domains and 6 DNS-style domains (ignored 1 non-domain entries)
[+] Sample of non-domain entries:
    - "0.0.0.0"
[+] List stages unchanged
[+] Target: https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts
[+] Status: Retrieval successful
[+] Server 11770: smart domains and 6 DNS-style domains (ignored 0 non-domain entries)
[+] Building tree
[+] Resolving domains
[+] The dns database remains available
[+] Number of gravity domains: 10117 (104942 unique domains)
[+] Number of smart blacklisted domains: 0
[+] Number of open blacklisted filters: 0
[+] Number of smart whitelisted domains: 0
[+] Number of open whitelisted filters: 0
[+] Flushing DNS cache
[+] Cleaning up stray entries
[+] PiH is listening on port 53
[+] UDP (IPv4)
[+] TCP (IPv4)
[+] UDP (IPv6)
[+] TCP (IPv6)
[+] Pi-hole blocking is enabled
root@firewall:~#
```

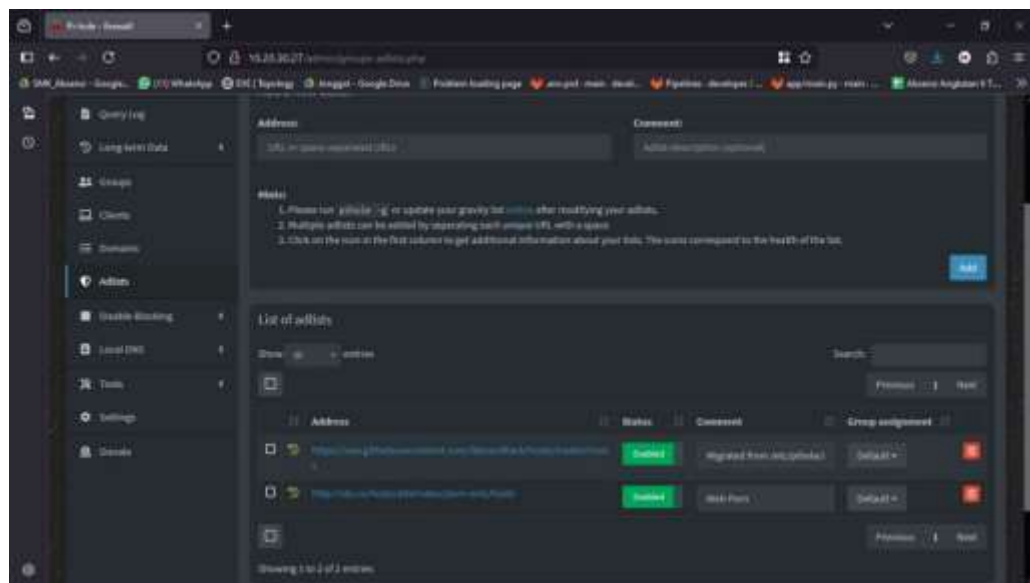
Gambar 3.1⁽¹⁾ Instalasi Pi hole pada Server



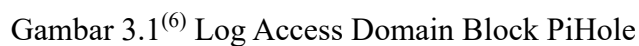
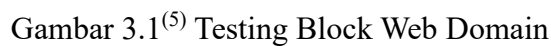
Gambar 3.1⁽²⁾ Dashboard system Pi-Hole



Gambar 3.1⁽³⁾ Addlist Domain Pihole



Gambar 3.1⁽⁴⁾ Addlist Domain Blocking



Implementasi sistem firewall adaptif di wilayah sekitar IDN Boarding School mendapat respon positif dari masyarakat, terutama dalam menciptakan lingkungan internet yang lebih aman bagi siswa dan warga sekitar. Orang tua dan guru merasa lebih tenang karena akses ke situs berbahaya dapat dibatasi, sementara masyarakat mengapresiasi langkah ini sebagai upaya



menjaga moral dan etika digital. Selain itu, kualitas penggunaan internet meningkat karena akses lebih terfokus pada aktivitas akademik dan produktif.

Namun, terdapat beberapa tantangan, seperti pemblokiran tidak disengaja terhadap situs edukatif serta upaya pengguna dalam melewati firewall menggunakan VPN atau DNS alternatif. Untuk mengatasi hal ini, sistem diperbarui dengan whitelist situs akademik serta konfigurasi tambahan guna mencegah bypass firewall. Meskipun ada kendala dalam sosialisasi kebijakan ini, secara keseluruhan masyarakat mendukung penerapan firewall sebagai langkah strategis dalam mengelola akses internet yang lebih bertanggung jawab dan sehat.

Pembahasan

Efektivitas Firewall dalam Memblokir Konten Negatif

Hasil penelitian menunjukkan bahwa penggunaan Pi-hole dan filter DNS efektif dalam membatasi akses ke situs pornografi. Metode filtering ini memiliki keunggulan dalam hal kecepatan eksekusi karena hanya bekerja pada tingkat DNS tanpa harus menganalisis konten dari setiap paket data yang masuk ke jaringan.

Namun, terdapat beberapa tantangan yang dihadapi dalam implementasi sistem ini, yaitu:

1. **False Blocking (Pemblokiran yang Tidak Diperlukan):** Beberapa situs edukatif yang menggunakan kata kunci yang mirip dengan situs berbahaya ikut terblokir.
 - **Solusi:** Penyusunan **whitelist** secara berkala untuk memastikan hanya situs yang benar-benar perlu diblokir yang masuk ke daftar pemfilteran.
2. **Bypass dengan VPN dan DNS Alternatif:** Pengguna yang lebih mahir mencoba menghindari firewall dengan menggunakan VPN atau DNS publik seperti Google DNS atau Cloudflare DNS.
 - **Solusi:** Sistem firewall dikonfigurasi untuk **memblokir akses ke layanan VPN**, serta memaksa semua permintaan DNS melalui sistem Pi-hole.

Dampak Implementasi terhadap Lingkungan Sekolah dan Masyarakat

Implementasi sistem firewall ini membawa dampak yang signifikan terhadap lingkungan IDN Boarding School dan masyarakat sekitar. Beberapa manfaat utama yang diperoleh dari sistem ini meliputi:

a. Bagi Siswa



- Mencegah akses ke konten pornografi yang dapat berdampak negatif pada perkembangan moral dan akademik mereka.
- Meningkatkan fokus dan produktivitas dalam belajar, karena akses internet hanya terbatas pada sumber yang relevan.

b. Bagi Guru dan Administrator Jaringan

- Memberikan kontrol lebih baik terhadap akses internet, sehingga dapat memastikan bahwa penggunaan jaringan sesuai dengan nilai pendidikan yang dianut sekolah.
- Mengurangi kekhawatiran terkait penyalahgunaan internet oleh siswa.

c. Bagi Masyarakat Sekitar

- Masyarakat yang menggunakan jaringan Wi-Fi sekolah mendapatkan akses internet yang lebih terkontrol, sehingga mengurangi risiko paparan konten negatif bagi anak-anak.
- Memberikan edukasi kepada masyarakat tentang pentingnya pengelolaan akses internet yang bertanggung jawab.

Potensi Pengembangan Lebih Lanjut

Meskipun sistem firewall ini telah menunjukkan hasil yang positif, terdapat beberapa aspek yang dapat dikembangkan lebih lanjut untuk meningkatkan efektivitas dan fleksibilitas sistem, antara lain:

1. Integrasi dengan Machine Learning

Penggunaan kecerdasan buatan (AI) dalam mendeteksi situs berbahaya berdasarkan pola akses pengguna, sehingga sistem dapat menyesuaikan daftar blokir secara otomatis tanpa perlu intervensi manual yang berulang.

2. Pemberlakuan Kebijakan Akses yang Berbeda untuk Setiap Pengguna

Saat ini, semua pengguna memiliki aturan pemblokiran yang sama. Pengembangan sistem berbasis user authentication memungkinkan pembuatan kebijakan akses yang lebih fleksibel, misalnya akses lebih luas bagi guru dan administrator dibandingkan siswa.

3. Dashboard Monitoring dan Laporan Penggunaan



Pengembangan sistem pemantauan berbasis dashboard analitik untuk melihat pola penggunaan internet, jumlah situs yang diblokir, dan upaya bypass yang dilakukan pengguna.

4. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian, sistem firewall adaptif yang dikembangkan telah terbukti efektif dalam membatasi akses ke situs pornografi di jaringan wilayah sekitar IDN Boarding School. Dengan tingkat pemblokiran lebih dari 95%, sistem ini berhasil menciptakan lingkungan internet yang lebih aman bagi siswa dan masyarakat sekitar tanpa mengganggu akses akademik.

Keberhasilan sistem ini menunjukkan bahwa metode Pi-hole dan DNS filtering dapat menjadi solusi yang efektif dan efisien untuk pengelolaan akses internet di lingkungan pendidikan. Namun, untuk meningkatkan efektivitas jangka panjang, sistem perlu dikembangkan lebih lanjut dengan teknologi machine learning, manajemen akses berbasis pengguna, serta fitur pemantauan jaringan yang lebih komprehensif.

Dengan implementasi yang lebih luas, sistem ini diharapkan dapat menjadi model bagi institusi pendidikan lain dalam mengelola keamanan jaringan dan menciptakan lingkungan digital yang lebih sehat dan bertanggung jawab.

DAFTAR PUSTAKA

- A. Alahmadi, R. Al-Shaer, and S. Jha, "Analysis and Evaluation of Network and Application Security Based on Next Generation Firewall," *International Journal of Network Security & Its Applications (IJNSA)*, vol. X, no. Y, pp. Z-Z, 202X.
- A. B. Pratomo, "Pengembangan Sistem Firewall pada Jaringan Komputer Berbasis Mikrotik RouterOS," *Bulletin of Network Engineering and Informatics*, vol. 1, no. 2, pp. 51-58, October 2023. DOI: 10.59688/bufnets.
- W. Styorini, H. Azwar, and M. Susantok, "Implementasi Firewall Pada Laboratorium Jaringan Komputer SMAIT AL-ITTIHAD," *Jurnal Inovasi Terapan Pengabdian Masyarakat (JITER-PM)*, vol. 2, no. 1, pp. 38-44, March 2024. DOI: 10.35143/jiter-pm.v2i1.6162.
- R. Permana, D. Ramadhani, and I. Lestari, "Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuruan Al-Madani Pontianak," *International Journal of Natural Sciences and Engineering*, vol. 3, no. 1, pp. 37-43, 2019.



- A. Ahmad & C. Sari, "Pengaruh Penggunaan Media Pembelajaran Berbasis Teknologi terhadap Hasil Belajar Siswa di Sekolah Menengah Atas," *Jurnal Pendidikan dan Teknologi*, vol. 2, no. 3, pp. 15-22, 2021.
- S. A. F. Rahman, "Implementasi Pendidikan Karakter dalam Kurikulum Sekolah Dasar," *Jurnal Pendidikan Indonesia*, vol. 5, no. 2, pp. 89-102, 2018.
- A. Budi & D. Citra, "Studi Pengaruh Penggunaan Teknologi Digital terhadap Pengembangan Pendidikan Islam," *Jurnal Pendidikan Islam*, vol. 3, no. 2, pp. 45-59, 2020.
- Adinda Setyaning Utami, 'Implikasi Yuridis Terhadap Privasi Akses Pornografi' (2023) Vol. 6 No. 4 *Jurist-Diction*.
- Rila Kusumaningsih & Suhardi, "Penanggulangan Pemberantasan Judi Online di Masyarakat," *ADMA: Jurnal Pengabdian dan Pemberdayaan Masyarakat*, vol. 4, no. 1, pp. 1-10, 2023. doi: 10.30812/adma.v4i1.2767.
- Herningtyas, R., Nurnisya, F. Y., & Ardiyanto, Y. (2021). Peningkatan Ketrampilan Parental Kontrol untuk Mengurangi Akses Pornografi Anak Bagi Pimpinan Ranting Aisyiyah. *WEBINAR ABDIMAS 4 - 2021: Inovasi Teknologi Tepat Guna dan Model Peningkatan Kapasitas Masyarakat Era Covid-19*, 147-156. DOI: 10.18196/ppm.41.805
- Purwanto, A., Ningtyias, F. W., & Ririanty, M. (2023). Niat Penghentian Akses Pornografi pada Remaja sebagai Upaya Pencegahan Perilaku Seksual Pranikah. *Ikesma: Jurnal Ilmu Kesehatan Masyarakat*, 19(1), 27-37. DOI: 10.19184/ikesma.v19i1.24336
- Ramadhani, I., Noer, M., & Mahardhika, M. I. (2023). Analisis Aplikasi Judi Online dari Segi Keamanan, Privasi, dan Etika dalam Perspektif Hukum Negara Indonesia. *Prosiding Seminar Nasional Teknologi dan Sistem Informasi (SITASI) 2023*, 542-552. ISSN: 2828-786X
- 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 Professionals*, 7(1), 27-38. E-ISSN: 2548-3412
- Muzakir, A., & Ulfa, M. (2019). Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan. *Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, 10(1), 15-20.
- I. Al Rasyid, "Parsing Data Log Hasil Pemblokiran Situs Negatif Di Satuan Kerja Perangkat Aceh," *Jurnal Teknologi dan Sistem Informasi*, vol. 10, no. 2, pp. 145–155, 2024.



- A. Smith, "A Study on Web Filtering and Content Blocking Mechanisms," *International Journal of Cyber Security*, vol. 12, no. 3, pp. 220–235, 2022.
- A. Setiawan, "Perancangan Sistem Keamanan Jaringan Berbasis Hierarchical Network Design," *Jurnal Keamanan Jaringan*, vol. 5, no. 1, pp. 33-42, 2023.
- N. Q. Buamona, M. Hamid, and E. Gunawan, "Analisis dan Implementasi Keamanan Jaringan Menggunakan Metode DHCP Snooping dan Switch Port Security," *Jurnal Teknologi Informatika (J-TIFA)*, vol. 6, no. 1, pp. 23-31, Mar. 2023. DOI: 10.52046/j-tifa.v6i2.1680.
- W. Hidayat and A. D. Yusuf, "Manajemen Penjadwalan Waktu Blokir Akses Internet pada Mikrotik RouterOS," *SCIENTIST: Journal of Security, Computer, Information, Embedded, Network, and Intelligence System*, vol. 1, no. 1, pp. 10–15, 2023. DOI: <https://journal.lontaradigitech.com/SCIENTIST>.
- 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 (JISAMAR)*, vol. 5, no. 2, pp. 340–349, May 2021. DOI: 10.52362/jisamar.v5i2.422.
- D. Zulkifli and Y. Yunita, "Implementasi Manajemen Bandwidth dan Blokir Website Dengan Address List Name di Mikrotik Pada CV Berkah Sumber Mas," *SATIN – Sains dan Teknologi Informasi*, vol. 8, no. 2, pp. 172–182, Dec. 2022. DOI: 10.33372/stn.v8i2.813.
- M. I. Saputra, "A Literature Review Network Security," *Jurnal Jaringan Komputer dan Keamanan*, vol. 4, no. 3, pp. 30–34, 2023. DOI: 10.61346/jjkk.v4i3.66.
- R. Setiawan, "Implementasi Zero Trust Architecture untuk Meningkatkan Keamanan Jaringan pada Perusahaan dengan Banyak Perangkat IoT," *Jurnal Ilmiah Penelitian dan Pembelajaran Informatika*, vol. 4, no. 1, pp. 1–10, 2024.
- A. Pratama, "Survei Penelitian Metode Kecerdasan Buatan untuk Mendeteksi Ancaman Siber," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 6, no. 2, pp. 123–135, 2023.
- D. Z. Rahman, "Analisa dan Perancangan Keamanan Jaringan Lokal Menggunakan Intrusion Prevention System," *Journal of Information System and Technology*, vol. 1, no. 2, pp. 45–55, 2020.



S. Nugroho, “Ancaman, Serangan, dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi,” Jurnal Pendidikan dan Aplikasi Industri, vol. 7, no. 2, pp. 61–70, 2020.