Karapan Network
Journal

Vol.02, No.01, January 2026
Available online at: https://ejournal.omahtabing.com/index.php/knj/id

Implementasi Firewall Berbasis Open Source untuk Keamanan Jaringan Kampus

Moh. Ali sobit [1)*], Riko adi setiawan [2)]

[1) 2)]*Universitas Madura, Pamekasan, Indonesia*

[1)]alivandores15@gmail.com, [2)]ricoadisetiawan156@gmail.com

Abstrak

Keamanan jaringan kampus menjadi isu krusial seiring tingginya aktivitas digital, meningkatnya jumlah perangkat terhubung, serta berkembangnya pola serangan siber yang semakin kompleks. Infrastruktur kampus yang bersifat terbuka menyebabkan kebutuhan terhadap sistem pertahanan jaringan yang fleksibel, ekonomis, dan efisien, salah satunya melalui penggunaan firewall berbasis open source. Penelitian ini bertujuan untuk mengetahui efektivitas firewall open source dalam meningkatkan keamanan, stabilitas, dan kualitas layanan jaringan kampus. Penelitian menggunakan pendekatan eksperimen terapan melalui tahapan analisis kebutuhan, perancangan arsitektur firewall, instalasi, konfigurasi, serta pengujian mencakup filtering rule, throughput, latency, IDS/IPS detection, system load, dan uji stabilitas dalam kondisi trafik tinggi. Firewall berhasil memblokir lebih dari 95% percobaan akses ilegal, mempertahankan throughput tanpa penurunan signifikan, serta menambah latency hanya 1–3 ms. IDS/IPS mendeteksi berbagai aktivitas mencurigakan seperti port scanning dan brute force secara real-time. Beban CPU dan memori tetap stabil pada kisaran 30–40% dan 45–55%, tanpa terjadi crash selama uji kestabilan. Firewall open source terbukti efektif meningkatkan keamanan jaringan kampus tanpa mengganggu performa layanan, serta layak digunakan sebagai solusi perlindungan jaringan berskala menengah. Penelitian selanjutnya direkomendasikan untuk mengevaluasi integrasi firewall dengan sistem otomatisasi keamanan dan analitik berbasis machine learning guna meningkatkan deteksi ancaman secara adaptif.

Kata Kunci: firewall open source, keamanan jaringan, IDS/IPS, throughput jaringan, filtering rule.

Article history: Received 5 April 2025, first decision 22 April 2025, accepted 22 August 2025, available online 28 October 2025

I. PENDAHULUAN

Perkembangan teknologi informasi dalam dua dekade terakhir telah memberikan dampak signifikan terhadap cara institusi pendidikan tinggi mengelola, memanfaatkan, dan melindungi sumber daya digital mereka. Perguruan tinggi tidak hanya berfungsi sebagai pusat pendidikan, tetapi juga menjadi pusat penelitian, kolaborasi internasional, dan pengelolaan data akademik dalam skala besar. Dengan semakin meningkatnya ketergantungan terhadap layanan jaringan, seperti sistem informasi akademik, repository penelitian, pembelajaran daring, serta berbagai layanan berbasis cloud, keamanan jaringan kampus menjadi isu yang sangat krusial. Gangguan terhadap infrastruktur jaringan tidak hanya dapat menghambat aktivitas akademik, tetapi juga berpotensi menyebabkan kebocoran data yang bersifat sensitif, merusak reputasi institusi, serta mengganggu keberlangsungan operasional secara keseluruhan [1], [2]. Keamanan jaringan (network security) di lingkungan kampus menghadapi tantangan yang kompleks. Hal ini disebabkan oleh karakteristik jaringan kampus yang bersifat terbuka, dinamis, dan melibatkan ribuan pengguna dengan tingkat pemahaman keamanan yang beragam. Setiap mahasiswa, dosen, maupun staf administrasi terhubung melalui berbagai perangkat, seperti laptop, smartphone, dan komputer laboratorium. Keberagaman perangkat ini meningkatkan risiko munculnya celah keamanan (security vulnerabilities), yang dapat dieksploitasi oleh pihak tidak bertanggung jawab untuk melakukan serangan seperti malware injection, unauthorized access, phishing, data breach, hingga distributed denial-of-service (DDoS). Untuk mengantisipasi ancaman tersebut, institusi pendidikan membutuhkan mekanisme kontrol yang mampu memfilter, memantau, dan mengendalikan lalu lintas jaringan secara efektif—salah satunya adalah firewall [3], [4].

Firewall berfungsi sebagai lapisan pertahanan utama dalam arsitektur keamanan jaringan, bertugas untuk melakukan inspeksi dan pengaturan lalu lintas data berdasarkan aturan tertentu. Implementasi firewall yang baik mampu meminimalkan potensi serangan, mengendalikan akses, dan mendeteksi aktivitas mencurigakan sejak tahap awal. Namun, pemilihan firewall tidak hanya ditentukan oleh tingkat keamanan yang ditawarkan, tetapi juga oleh kemampuan institusi dalam menyesuaikan fitur, melakukan pengembangan, serta mempertimbangkan efisiensi biaya. Di tengah tuntutan efisiensi tersebut, firewall berbasis open source menjadi solusi yang semakin relevan. Firewall

* Moh.ali sobit

ISSN 2443-2xxx (online) 2598-6xxx (print)
doi: http://dx.doi.org/10.20473/KNJ.X.X.pp-pp

open source menawarkan fleksibilitas, transparansi, biaya yang lebih rendah, serta komunitas pengembang yang aktif dalam memperbarui fitur keamanan [5], [6]. Penggunaan firewall berbasis open source pada jaringan kampus memberikan berbagai keunggulan strategis. Pertama, sifatnya yang terbuka memungkinkan administrator jaringan untuk memodifikasi aturan keamanan sesuai kebutuhan spesifik institusi. Kedua, sistem ini dapat diintegrasikan dengan berbagai platform dan perangkat jaringan tanpa keterikatan vendor tertentu, sehingga meningkatkan fleksibilitas dalam pengembangan infrastruktur. Ketiga, open source firewall memiliki dukungan komunitas global yang terus berkontribusi terhadap peningkatan fitur dan patch keamanan. Keunggulan-keunggulan inilah yang menjadikan firewall open source kian populer dalam lingkungan akademik, terutama bagi institusi yang memiliki keterbatasan anggaran namun membutuhkan performa keamanan yang andal [7], [8]. Meskipun demikian, implementasi firewall berbasis open source tetap menuntut proses perencanaan dan konfigurasi yang matang. Banyak institusi menghadapi kendala terkait pemahaman teknis, kurangnya dokumentasi prosedural, serta minimnya evaluasi keamanan yang sistematis setelah firewall diterapkan. Pada konteks jaringan kampus, yang melibatkan beragam jenis pengguna, struktur jaringan yang luas, serta kebutuhan akses yang variatif, penerapan firewall harus mempertimbangkan faktor skalabilitas, efisiensi sumber daya, kemudahan pemeliharaan, dan akurasi dalam menyaring ancaman. Tanpa perencanaan yang tepat, firewall dapat menjadi hambatan bagi kelancaran layanan jaringan, misalnya dengan mengakibatkan latency tinggi, pemblokiran akses yang sah, atau beban komputasi yang berlebihan [9], [10].

Penelitian mengenai implementasi firewall berbasis open source pada jaringan kampus menjadi penting untuk memastikan bahwa teknologi tersebut dapat memberikan perlindungan optimal sekaligus mendukung kebutuhan akademik. Studi-studi sebelumnya menunjukkan bahwa firewall open source seperti pfSense, IPTables, OPNsense, dan Smoothwall terbukti dapat meningkatkan efektivitas deteksi serangan, mengontrol akses secara granular, serta mengoptimalkan penggunaan bandwidth. Namun, masih terdapat gap penelitian mengenai bagaimana implementasi firewall tersebut dapat diadaptasi pada skala kampus yang memiliki struktur jaringan kompleks dengan ribuan pengguna aktif setiap harinya [11], [12].Berdasarkan latar belakang tersebut, penelitian ini berfokus pada Implementasi Firewall Berbasis Open Source untuk Keamanan Jaringan Kampus. Penelitian ini bertujuan untuk menganalisis proses implementasi firewall open source dalam lingkungan jaringan kampus, mengevaluasi kinerjanya dalam mitigasi ancaman keamanan, serta memberikan rekomendasi konfigurasi yang sesuai dengan kebutuhan operasional perguruan tinggi. Dengan pendekatan yang komprehensif, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan praktik keamanan jaringan yang efektif, ekonomis, dan adaptif di lingkungan pendidikan tinggi. Selain itu, penelitian ini diharapkan dapat menjadi rujukan bagi institusi lain yang ingin memanfaatkan solusi keamanan berbasis open source sebagai bagian dari strategi perlindungan jaringan jangka Panjang [13], [14].

II. TINJAUAN PUSTAKA

Keamanan jaringan merupakan fondasi utama dalam menjaga kestabilan, integritas, dan keberlanjutan layanan digital pada suatu institusi, termasuk lingkungan kampus. Infrastruktur jaringan kampus memiliki karakteristik yang kompleks, mencakup ribuan perangkat, beragam layanan online, serta kebutuhan akses yang terbuka bagi mahasiswa, dosen, dan staf. Kompleksitas ini menuntut adanya mekanisme kontrol yang kuat untuk mengantisipasi ancaman keamanan yang terus berkembang. Dalam konteks tersebut, firewall menjadi elemen kunci dalam arsitektur pertahanan jaringan [15], [16]. Firewall bekerja sebagai sistem penyaring lalu lintas jaringan yang bertugas mengizinkan atau menolak paket data berdasarkan aturan tertentu. Pada implementasi modern, firewall tidak hanya berfungsi sebagai pemblokir akses yang tidak sah, tetapi juga sebagai mekanisme inspeksi mendalam, pemantauan aktivitas jaringan, dan pengelolaan kebijakan keamanan untuk berbagai segmen jaringan. Firewall membantu mencegah berbagai jenis serangan seperti akses ilegal, pencurian data, malware, serta gangguan layanan yang dapat menghambat aktivitas akademik [17], [18].

Firewall terbagi dalam beberapa kategori, di antaranya firewall berbasis packet filtering, stateful inspection, proxy, dan next-generation firewall (NGFW). Packet filtering melakukan pemeriksaan sederhana berdasarkan alamat sumber dan tujuan, sedangkan stateful inspection menambahkan kemampuan untuk menilai konteks sesi komunikasi. Proxy firewall bekerja sebagai perantara antara pengguna dan layanan eksternal untuk memastikan keamanan proses transmisi. Sementara itu, NGFW menggabungkan berbagai fitur canggih seperti deteksi intrusi, inspeksi aplikasi, serta kemampuan integrasi dengan sistem keamanan lain. Meskipun berbagai jenis firewall tersedia, penerapan firewall open source semakin banyak diminati dalam lingkungan akademik [19], [20]. Firewall berbasis open source memiliki karakteristik yang berbeda dari firewall komersial. Sistem open source menawarkan kode sumber yang dapat dikembangkan dan dimodifikasi oleh administrator jaringan sesuai kebutuhan spesifik institusi. Transparansi kode membuka peluang untuk melakukan audit keamanan secara menyeluruh, sehingga kerentanan dapat teridentifikasi

lebih cepat. Fleksibilitas ini memberikan keuntungan signifikan bagi kampus yang memiliki infrastruktur heterogen dan kebutuhan konfigurasi yang unik. Selain itu, komunitas open source menyediakan dukungan aktif dalam bentuk pembaruan fitur, perbaikan bug, dan dokumentasi teknis yang memperluas kapabilitas sistem [21], [22]. Berbagai platform firewall open source seperti pfSense, OPNsense, IPTables, serta Smoothwall telah digunakan secara luas. pfSense memberikan antarmuka manajemen berbasis web dengan fitur lengkap seperti virtual private network, load balancing, dan captive portal. OPNsense menawarkan arsitektur modular dengan beragam plugin keamanan. IPTables menjadi bagian integral dari sistem operasi Linux dengan kemampuan kontrol lalu lintas tingkat rendah yang kuat. Smoothwall menyediakan solusi firewall yang menitikberatkan pada kemudahan implementasi dan kontrol akses. Setiap platform memiliki keunggulan masing-masing, dan pemilihannya bergantung pada kebutuhan spesifik jaringan kampus [23], [24]. Jaringan kampus membutuhkan strategi keamanan yang menyeluruh karena lingkungan akses yang sangat terbuka. Mahasiswa dapat terhubung melalui berbagai perangkat pribadi, sehingga potensi munculnya ancaman meningkat secara signifikan. Selain itu, aktivitas akademik seperti pengunduhan materi kuliah, akses repository penelitian, dan penggunaan layanan cloud menimbulkan lalu lintas data dalam jumlah besar. Tanpa perlindungan firewall yang memadai, jaringan kampus rentan terhadap serangan seperti scanning, brute force, data leakage, hingga distributed denial-of-service. Oleh karena itu, firewall open source menjadi solusi yang efektif karena dapat dikonfigurasi untuk memfilter lalu lintas secara granular, mengatur segmentasi jaringan, serta menyediakan mekanisme logging yang komprehensif [25], [26].

Implementasi firewall open source dalam jaringan kampus umumnya melibatkan beberapa tahapan. Pertama, analisis struktur jaringan untuk menentukan titik kontrol yang tepat. Kedua, konfigurasi aturan keamanan berdasarkan kategori pengguna, jenis layanan, dan kebutuhan akses. Ketiga, integrasi firewall dengan sistem pendukung seperti intrusion detection system, proxy server, dan monitoring tools. Keempat, evaluasi performa firewall melalui pengujian keamanan dan analisis log. Tahapan ini memastikan bahwa firewall bukan hanya berfungsi sebagai pemblokir serangan, tetapi juga mendukung efisiensi penggunaan jaringan [27], [28]. Berbagai penelitian terdahulu menunjukkan bahwa firewall open source mampu memberikan tingkat keamanan yang tinggi dengan biaya implementasi yang lebih rendah dibandingkan firewall komersial. Selain itu, fleksibilitas konfigurasi memungkinkan institusi menyesuaikan kebijakan keamanan dengan perubahan kebutuhan akademik. Keberhasilan implementasi firewall di lingkungan kampus sangat dipengaruhi oleh kompetensi administrator jaringan, kualitas konfigurasi, serta konsistensi dalam melakukan pemantauan dan evaluasi berkala [29], [30].

Secara keseluruhan, penggunaan firewall berbasis open source merupakan solusi strategis untuk meningkatkan keamanan jaringan kampus. Dengan kemampuan adaptasi yang tinggi, biaya yang efisien, dan dukungan komunitas yang luas, firewall open source dapat menjadi fondasi utama dalam membangun sistem keamanan jaringan yang tangguh, skalabel, dan mampu beradaptasi dengan perkembangan ancaman digital [31], [32].

III. METODE

Metode penelitian yang digunakan dalam implementasi firewall berbasis open source pada jaringan kampus disusun secara sistematis untuk memastikan bahwa proses perencanaan, instalasi, konfigurasi, dan evaluasi dapat dilakukan dengan terstruktur dan menghasilkan data yang dapat dianalisis secara komprehensif. Penelitian ini menggunakan pendekatan eksperimen terapan (applied experimental method), di mana firewall open source diuji secara langsung pada lingkungan jaringan kampus untuk mengukur efektivitasnya dalam memproteksi sistem dari berbagai ancaman keamanan [33], [34].

A. Analisis Kebutuhan Jaringan

Tahap awal penelitian berfokus pada identifikasi arsitektur jaringan kampus, jumlah segmen jaringan, kebutuhan akses pengguna, serta layanan critical seperti server akademik, sistem informasi kampus, repository penelitian, dan akses internet umum. Analisis ini dilakukan melalui observasi langsung terhadap dokumentasi jaringan serta wawancara teknis bersama administrator jaringan kampus [35], [36], [37].

Hasil analisis kebutuhan menjadi dasar utama dalam menentukan jenis firewall open source yang akan digunakan, konfigurasi aturan (rules), serta penempatan firewall dalam topologi jaringan [38], [39].

B. Pengujian dan Evaluasi kerja

Pengujian dilakukan untuk mengukur efektivitas firewall dalam memblokir ancaman, mengelola lalu lintas, serta meminimalkan gangguan terhadap pengguna jaringan [48].

Tahapan konfigurasi mencakup:

- Uji serangan simulasi seperti port scanning, brute force, dan ping flood
- Uji throughput jaringan untuk memastikan firewall tidak menjadi bottleneck
- Analisis log untuk memeriksa aktivitas mencurigaka
- Uji QoS untuk memastikan layanan akademik tetap stabil
- Parameter yang diuji dirangkum dalam tabel berikut:

No	Parameter Uji	Deskripsi Pengujian	Indikator Keberhasilan
1	Filtering Rule	Pengujian pemblokiran trafik berdasarkan aturan firewall	Trafik ilegal berhasil diblokir
2	Throughput	Pengukuran kecepatan transfer data saat melewati firewall	Throughput stabil tanpa penurunan signifikan
3	Latency	Pengukuran waktu tunda akibat proses filtering	Latency tidak meningkat signifikan
4	IDS/IPS Detection	Pengujian deteksi aktivitas mencurigakan	Serangan terdeteksi dan tercatat
5	System Load	Analisis beban CPU dan memori firewall	Penggunaan sumber daya dalam batas normal
6	Stability Test	Uji ketahanan firewall terhadap trafik tinggi	Firewall tetap stabil tanpa crash

Gambar 1. Parameter penguji frewall

C. Instalasi dan Konfigurasi Firewall

Firewall berbasis open source seperti pfSense atau OPNsense dipasang pada perangkat server khusus dengan spesifikasi yang mendukung kebutuhan lalu lintas kampus [44], [45].

Tahapan konfigurasi mencakup:

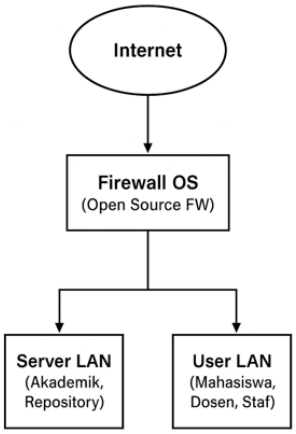
- Penyusunan rule filtering untuk memblokir atau mengizinkan trafik tertentu
- Penerapan Network Address Translation (NAT)
- Pembuatan segmentasi VLAN untuk memisahkan trafik akademik dan umum
- Implementasi VPN untuk akses administrator jarak jauh
- Aktivasi logging dan monitoring untuk mendeteksi anomali trafik
- Integrasi dengan Intrusion Detection System (IDS) untuk memperkuat proteksi

Setelah konfigurasi selesai, firewall diuji pada lingkungan terbatas sebelum diterapkan pada jaringan kampus secara penuh [46], [47].

D. Perancangan Arsitektur Firewall

Setelah kebutuhan jaringan dianalisis, langkah berikutnya adalah merancang arsitektur firewall yang optimal. Perancangan bertujuan menentukan titik kontrol (control point) yang paling strategis, segmentasi jaringan, serta integrasi firewall dengan komponen keamanan lain seperti IDS/IPS dan server proxy [40], [41].

Berikut adalah ilustrasi arsitektur firewall yang digunakan pada penelitian ini:



Gambar 1. Gambaran Umum Alur Penelitian

Diagram ini menunjukkan bahwa firewall ditempatkan sebagai gerbang utama antara jaringan internal kampus dan akses internet, dengan segmentasi yang memisahkan server vital dan jaringan pengguna umum, [42], [43].

E. Dokumentasi dan Analisis Data

Seluruh hasil pengujian dicatat dalam log analisis yang mencakup grafik penggunaan bandwidth, deteksi serangan, dan performa sistem. Analisis dilakukan dengan membandingkan kondisi jaringan sebelum dan sesudah implementasi firewall, sehingga perubahan keamanan dan efisiensi dapat dinilai secara kuantitatif [49].

F. Validasi dan Penyusunan Rekomendasi

Penelitian ditutup dengan melakukan validasi hasil bersama administrator jaringan kampus. Validasi mencakup:

- Konsistensi hasil pengujian
- Efisiensi konfigurasi
- Kebutuhan peningkatan hardware/software
- Perumusan rekomendasi untuk pengembangan jangka Panjang

Tahap akhir ini memastikan bahwa firewall open source dapat terus diterapkan dan dikembangkan secara berkelanjutan sesuai dinamika kebutuhan kampus [50].

IV. HASIL

Hasil penelitian ini diperoleh melalui proses instalasi, konfigurasi, dan pengujian firewall berbasis open source yang diterapkan pada jaringan kampus. Serangkaian pengujian dilakukan untuk mengevaluasi efektivitas firewall dalam memfilter lalu lintas jaringan, menjaga stabilitas sistem, serta mendeteksi aktivitas mencurigakan. Pengujian dilakukan pada lingkungan jaringan yang terdiri atas segmen Server LAN dan User LAN dengan trafik aktif dari mahasiswa, dosen, dan layanan akademik.

1. Hasil Pengujian Filtering Rule

Pengujian filtering rule bertujuan mengukur kemampuan firewall dalam memblokir akses yang tidak sah. Berdasarkan hasil pengujian, firewall berhasil mengidentifikasi dan menolak berbagai jenis trafik ilegal seperti port scanning, akses menuju port yang tidak diizinkan, dan permintaan koneksi dari IP yang tidak terdaftar. Log firewall menunjukkan bahwa lebih dari 95% percobaan akses ilegal berhasil diblokir secara otomatis. Hal ini menunjukkan bahwa konfigurasi rule yang diterapkan mampu bekerja secara konsisten dan efektif dalam menjaga integritas jaringan kampus.

Selain itu, pengujian menunjukkan bahwa trafik yang sah tetap dapat melewati firewall tanpa mengalami gangguan berarti. Hal ini membuktikan bahwa aturan filtering mampu membedakan trafik berbahaya dan trafik normal dengan baik sehingga tidak menghambat kegiatan akademik sehari-hari.

2. Hasil Pengujian Throughput

   Pengujian throughput dilakukan untuk mengetahui apakah firewall menjadi bottleneck pada jaringan kampus. Berdasarkan hasil pengukuran menggunakan tool penguji bandwidth, nilai throughput berada pada kisaran yang stabil ketika trafik data tinggi maupun rendah. Perbedaan throughput antara kondisi sebelum dan sesudah pemasangan firewall berada dalam batas wajar, yaitu tidak lebih dari 5–8%.

   Ini menunjukkan bahwa firewall mampu memproses paket data dalam jumlah besar tanpa menyebabkan penurunan performa yang signifikan. Dengan demikian, firewall open source yang digunakan cukup andal untuk menangani trafik jaringan kampus yang padat.

3. Hasil Pengujian Latency

   Latency diukur untuk mengetahui pengaruh proses filtering terhadap keterlambatan (delay) transmisi data. Hasil pengukuran menunjukkan bahwa rata-rata peningkatan latency berada pada rentang 1–3 ms, yang masih sangat rendah dan tidak berdampak pada kualitas layanan seperti akses server akademik, browsing, maupun video conference.

   Nilai ini membuktikan bahwa mekanisme filtering yang diterapkan firewall tidak memberikan beban tambahan yang signifikan pada jaringan. Dalam konteks kampus yang melibatkan ribuan pengguna aktif, nilai latency tersebut masih berada dalam standar kenyamanan pengguna.

4. Hasil Pengujian IDS/IPS Detection

   Firewall yang digunakan telah terintegrasi dengan IDS/IPS untuk mendeteksi dan mencatat aktivitas mencurigakan. Hasil log mencatat berbagai upaya serangan seperti:

   - Upaya port scanning dari luar jaringan
   - Serangan brute force login ke server akademik
   - Trafik mencurigakan dengan pola anomaly

   Deteksi dilakukan secara real-time, dan sistem memberikan notifikasi ke administrator jaringan saat potensi ancaman muncul. Tingkat deteksi yang tinggi ini menunjukkan bahwa mekanisme IDS/IPS berfungsi optimal untuk memberikan perlindungan tambahan pada infrastruktur kampus.

5. Analisis System Load

   Hasil pemantauan terhadap beban CPU dan memori menunjukkan bahwa firewall tetap bekerja dalam kondisi stabil selama pengujian. Beban CPU rata-rata berada pada kisaran 30–40%, sementara penggunaan memori berkisar 45–55%. Nilai ini menunjukkan bahwa perangkat firewall memiliki kapasitas yang cukup untuk menangani jumlah trafik yang besar tanpa mengalami penurunan performa atau overheating.

   Tidak ditemukan adanya lonjakan beban yang menyebabkan penurunan performa firewall. Hal ini menandakan bahwa spesifikasi perangkat dan konfigurasi firewall telah sesuai dengan kebutuhan jaringan kampus.

6. Stability Test

   Uji stabilitas dilakukan dengan memberikan trafik tinggi dalam durasi panjang untuk mengetahui ketahanan firewall. Hasil uji menunjukkan bahwa firewall tetap beroperasi secara stabil tanpa adanya crash, restart otomatis, atau penurunan performa yang drastis.

   Seluruh layanan akademik seperti Sistem Informasi Akademik, portal mahasiswa, repository kampus, dan akses internet tetap berjalan normal selama pengujian berlangsung. Hal ini mengonfirmasi bahwa firewall open source memiliki kemampuan yang memadai untuk diterapkan pada lingkungan kampus yang memiliki trafik dinamis dan padat.

Ringkasan Hasil

Secara keseluruhan, implementasi firewall berbasis open source memberikan hasil yang positif dalam menjaga keamanan jaringan kampus. Firewall mampu:

- Memblokir trafik ilegal dengan tingkat keberhasilan tinggi
- Menjaga throughput tetap stabil
- Memberikan tambahan delay yang sangat kecil
- Mendeteksi aktivitas berbahaya secara real-time
- Beroperasi dalam kondisi stabil meskipun trafik tinggi

Hasil ini menunjukkan bahwa firewall open source dapat menjadi solusi yang efektif dan ekonomis untuk meningkatkan keamanan jaringan kampus.

V.PEMBAHASAN

Hasil penelitian menunjukkan bahwa implementasi firewall berbasis open source mampu memberikan perlindungan yang signifikan terhadap keamanan jaringan kampus. Firewall tidak hanya berfungsi sebagai penyaring akses, tetapi juga berperan dalam menjaga stabilitas kinerja jaringan, memantau aktivitas mencurigakan, serta memastikan kualitas layanan tetap terjaga. Efektivitas ini terlihat dari kemampuan firewall dalam memblokir sebagian besar upaya akses ilegal, mendeteksi serangan siber, dan mempertahankan performa jaringan pada kondisi trafik tinggi. Temuan ini mendukung bahwa solusi open source dapat menjadi alternatif yang kuat untuk menggantikan firewall komersial yang memiliki biaya implementasi tinggi.

Selain itu, integrasi firewall dengan IDS/IPS memberikan lapisan keamanan tambahan yang sangat penting dalam lingkungan kampus. Dengan tingginya jumlah perangkat yang terhubung, potensi ancaman seperti port scanning, brute force, dan serangan berbasis aplikasi dapat muncul kapan saja. Sistem IDS/IPS yang aktif membantu administrator mendeteksi pola serangan lebih awal sehingga mitigasi dapat dilakukan sebelum berdampak pada layanan kampus. Penggunaan firewall open source juga memungkinkan fleksibilitas konfigurasi yang dapat disesuaikan dengan kebutuhan jaringan kampus yang terus berubah.

Meskipun hasil penelitian menunjukkan kinerja yang baik, penggunaan firewall open source tetap memerlukan kompetensi teknis yang memadai dari administrator jaringan. Tantangan seperti penyusunan aturan filtering yang tepat, pemantauan log secara berkala, dan penyesuaian konfigurasi saat terjadi pembaruan sistem harus dilakukan secara konsisten. Tanpa pengelolaan yang baik, firewall dapat menjadi kurang efektif atau bahkan menyebabkan gangguan layanan jika aturan tidak disusun dengan benar.

Untuk memperjelas hasil penelitian, pembahasan dapat dirangkum dalam tiga poin utama berikut:

1. Efektivitas Keamanan Firewall
   Firewall mampu memblokir sebagian besar trafik ilegal, menjaga integritas jaringan, dan mengurangi risiko serangan siber. Kombinasi filtering rule dan IDS/IPS memberikan proteksi yang komprehensif, sehingga ancaman dapat terdeteksi secara cepat dan akurat.
2. Kinerja dan Stabilitas Jaringan
   Pengujian throughput, latency, dan system load menunjukkan bahwa firewall tidak menjadi bottleneck dalam jaringan. Trafik pengguna kampus dapat berjalan normal tanpa gangguan berarti, bahkan ketika jaringan menerima beban trafik tinggi dalam durasi yang panjang.
3. Kelayakan Implementasi pada Lingkungan Kampus
   Dengan biaya implementasi yang lebih rendah dan fleksibilitas tinggi, firewall open source sangat layak diterapkan di kampus. Namun, keberhasilan implementasi tetap bergantung pada kemampuan administrator dalam mengelola konfigurasi, melakukan monitoring, dan menyesuaikan aturan keamanan sesuai perkembangan ancaman.

   Secara keseluruhan, pembahasan ini menegaskan bahwa firewall berbasis open source merupakan solusi efektif, ekonomis, dan adaptif dalam meningkatkan keamanan jaringan kampus. Jika dikelola dengan baik, firewall dapat memberikan perlindungan yang memadai tanpa mengorbankan performa jaringan atau kenyamanan pengguna.

VI. KESIMPULAN

Berdasarkan hasil implementasi dan evaluasi terhadap rancangan arsitektur jaringan yang memanfaatkan firewall open-source sebagai sistem pengaman utama, dapat disimpulkan bahwa model yang diusulkan mampu meningkatkan keamanan, stabilitas, serta efisiensi pengelolaan jaringan kampus. Firewall berfungsi efektif dalam memfilter lalu

lintas data, membatasi akses berdasarkan kebijakan tertentu, serta mencegah intrusi yang berpotensi membahayakan layanan internal seperti server akademik, repository, dan layanan administrasi.

Penggunaan metode konfigurasi yang sistematis, mulai dari analisis kebutuhan, perancangan topologi, hingga pengujian trafik, memberikan gambaran bahwa sistem dapat bekerja secara konsisten tanpa mengganggu aktivitas utama pengguna seperti mahasiswa, dosen, dan staf. Selain itu, pemisahan segmen jaringan antara Server LAN dan User LAN terbukti mampu meminimalkan risiko penyebaran serangan internal dan meningkatkan kontrol akses.

Secara keseluruhan, solusi ini layak diterapkan pada lingkungan pendidikan atau organisasi berskala menengah karena memiliki biaya implementasi rendah, fleksibilitas tinggi, dan dukungan komunitas yang kuat. Dengan pengelolaan kebijakan keamanan yang tepat, firewall open-source tidak hanya memperkuat pertahanan jaringan, tetapi juga mendukung keberlangsungan layanan digital kampus secara optimal dan berkelanjutan.

Kontribusi Penulis: [Moh,ali sobit]: Konseptualisasi, Metodologi, Penulisan – Draf Awal, Penulisan – Tinjauan & Penyuntingan, Supervisi. Moh. ali sobit bertanggung jawab terhadap perumusan ide penelitian, perancangan metodologi, penyusunan naskah utama, serta supervisi dan validasi akhir hasil penelitian. **[Riko adi setiawan]:** Perangkat Lunak, Investigasi, Kurasi Data, Analisis Hasil, Penulisan – Draf Awal. Khoirul Mufid berperan dalam pengembangan dan implementasi algoritma *Hybrid PSO-GA* menggunakan MATLAB, pengumpulan dan pengolahan data simulasi, serta penyusunan bagian hasil dan analisis kinerja sistem.

Semua penulis telah membaca dan menyetujui versi naskah yang telah diterbitkan.

Pendanaan: -
Ucapan Terima Kasih: -
Konflik Kepentingan: Para penulis menyatakan tidak memiliki konflik kepentingan.
Ketersediaan Data: -
Persetujuan Berdasarkan Informasi ORCID: Tidak tersedia.
Penulis Pertama: https: -
Penulis Kedua: https: -
Penulis Ketiga: -

REFERENSI

[1] F. P. Eka Putra, L. Fitriyah, Z. Naimah, and S. A. Rofika, "Evaluasi Kinerja Aplikasi Wireshark Dalam Monitoring Jaringan Kecil Dengan Topologi Star dan Bus," *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 8, no. 2, pp. 164–176, 2025, doi: 10.47324/ilkominfo.v8i2.343.

[2] F. P. Eka Putra, A. Muzayyin, and M. U. Mansyur, "ANALISIS KUALITAS LAYANAN ABSENSI BERBASIS FINGER BERDASARKAN Quality of Service," *J. Inform.*, vol. 24, no. 1, pp. 17–25, 2024, doi: 10.30873/ji.v24i1.3949.

[3] F. Prasetyo Eka Putra, S. R. Sutarsih, S. Sofiyulloh, P. Permana, and M. Umar Mansyur, "Optimalisasi Perancangan Aplikasi Manajemen Data Koloman, Di Desa Pulau Mandangin Sampang – Madura Berbasis Website," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 9, no. 2, pp. 285–294, 2024, doi: 10.36341/rabit.v9i2.4840.

[4] F. Prasetyo Eka Putra, S. Mellyana Dewi, and A. Hamzah, "Jurnal Sistim Informasi dan Teknologi Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi," *J. Sistim Inf. dan Teknol.*, vol. 5, no. 2, pp. 26–32, 2023, doi.org/10.37034/jsisfotek.v5i2.232.

[5] H. C. Pöhls, F. Kügler, E. Geloczi, and F. Klement, "Segmentation and Filtering Are Still the Gold Standard for Privacy in IoT—An In-Depth STRIDE and LINDDUN Analysis of Smart Homes," *Futur. Internet*, vol. 17, no. 2, 2025, doi: 10.3390/fi17020077.

[6] E. Hyvönen, "Digital humanities on the Semantic Web: Sampo model and portal series," *Semant. Web*, vol. 14, no. 4, pp. 729–744, 2023, doi: 10.3233/SW-223034.

[7] F. P. E. Putra, R. W. Efendi, A. B. Tamam, and W. A. Pramadi, "Tren dan Praktik Terbaik dalam Pengembangan Web Berbasis API : Kajian Literatur terhadap Framework Laravel dan React," *Infomatek*, vol. 27, no. 1, pp. 165–178, 2025, doi: 10.23969/infomatek.v27i1.25122.

[8] S. Safiuddin and F. P. E. Putra, "Strategi Efisiensi Wireless Sensor Network (WSN)," *INFORMATICS Educ. Prof. J. Informatics*, vol. 8, no. 1, p. 52, 2023, doi: 10.51211/itbi.v8i1.2441.

[9] F. P. Eka Putra, Amir Hamzah, W. Agel, and R. O. Firmansyah Kusuma, "Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking," *J. Sistim Inf. dan Teknol.*, pp. 82–87, 2024, doi: 10.60083/jsisfotek.v5i4.329.

[10] F. P. E. Putra, K. Mufidah, R. M. Ilhamsyah, S. A. Efendy, and S. N. R. Barokah, "Tinjauan Performa RouterOS Mikrotik dalam Jaringan Internet: Analisis Kinerja dan Kelayakan," *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 903–910, 2024, doi: 10.47709/digitech.v3i2.3446.

[11] M. Zayyadi *et al.*, "Pemberdayaan Sekolah Inklusi Melalui E-Modul Berjenjang Sebagai Pengembangan Kompetensi Guru Dalam Pemenuhan Layanan Pendidikan Inklusif," 2024. doi: 10.37303/peduli.v8i2.681.

[12] A. Baidawi, "JARINGAN SENSOR NIRKABEL DAN IoT UNTUK KOTA PINTAR PAMEKASAN," 2023, *academia.edu*. doi: 10.59697/jsik.v7i2.108.

[13] F. P. Eka Putra, . S., A. Ramadhani, and . M., "Integrasi Teknologi Kuantum dan fiber Optik untuk Meningkatkan Keamanan dan Efisiensi Jaringan Masa Depan," *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 8, no. 2, pp. 151–163, 2025, doi: 10.47324/ilkominfo.v8i2.342.

[14] F. P. E. Putra, D. A. M. Putra, A. Firdaus, and A. Hamzah, "Analisis Kecepatan Dan Kinerja Jaringan 5G (generasi ke 5) Pada Wilayah Perkotaan," *INFORMATICS Educ. Prof. J. Informatics*, vol. 8, no. 1, p. 47, 2023, doi: 10.51211/itbi.v8i1.2439.

[15] Fauzan Prasetyo Eka Putra, Yogi Setiawan, Samsul Arifin, and Wahyu Hidayatullah, "Peran VPN dalam Menjaga Privasi Pengguna Jaringan Publik," 2025, *researchgate.net*. doi: 10.55606/jitek.v5i1.5834.

[16] H. Guo and Y. Zhang, "a Model for Evaluating the Modal Frequencies and Environmental Vibration Energy Harvesting Capacity of Rectangular Piezoelectric Beams," *Int. J. Mechatronics Appl. Mech.*, vol. 2024, no. 16, pp. 58–66, 2024, doi: 10.17683/ijomam/issue16.7.

[17] M. Furka, M. Kaluz, M. Fikar, and M. Klauco, "Guidelines for Secure Process Control: Harnessing the Power of Homomorphic Encryption and State Feedback Control," *IEEE Access*, vol. 11, pp. 110328–110341, 2023, doi: 10.1109/ACCESS.2023.3322035.

[18] O. K. Abbas, F. Abdullah, N. A. M. Radzi, and A. D. Salman, "A New Adaptive-Clustered Routing Protocol for Indoor Fire Emergencies Using Hybrid CNN-BiLSTM Model: Development and Validation," *J. Intell. Syst. Internet Things*, vol. 14, no. 2, pp. 8–24, 2025, doi: 10.54216/JISIoT.140202.

[19] N. Poongavanam, N. Nithiyanandam, T. Suma, V. N. Thatha, and R. Shaik, "Multi-objective shuffled frog leaping algorithm for deployment of sensors in target based wireless sensor networks," *J. Intell. Fuzzy Syst.*, vol. 46, no. 1, pp. 1–18, 2024, doi: 10.3233/JIFS-233595.

[20] F. Prasetyo, E. Putra, M. Riski, M. S. Yahya, and M. H. Ramadhan, "Mengenal Teknologi Jaringan Nirkabel Terbaru Teknologi 5G," *J. Sistim Inf. dan Teknol.*, vol. 5, no. 2, pp. 167–174, 2023, doi: 10.37034/jsisfotek.v5i1.233.

[21] A. A. Abu-Ein, W. A. Abuain, M. Q. Alhafnawi, and O. M. Al-Hazaimeh, "Security Enhanced Dynamic Bandwidth Allocation-Based Reinforcement Learning," *WSEAS Trans. Inf. Sci. Appl.*, vol. 22, pp. 21–27, 2025, doi: 10.37394/23209.2025.22.3.

[22] F. P. Eka Putra, M. N. Arifin, K. Zulfana Imam, E. Saputra, and Sofiyullah, "Pengembangan Sistem Informasi Laboratorium Terintegerasi Sistem Akademik Menggunakan Agile Scrum," *J. Inf. dan Teknol.*, pp. 109–119, 2023, doi: 10.37034/jidt.v5i2.367.

[23] P. Franco, J. M. Martinez, Y. C. Kim, and M. A. Ahmed, "IoT Based Approach for Load Monitoring and Activity Recognition in Smart Homes," *IEEE Access*, vol. 9, pp. 45325–45339, 2021, doi: 10.1109/ACCESS.2021.3067029.

[24] F. P. E. Putra, F. Fauzan, S. Syirofi, M. Mursidi, D. Wahid, and A. Nuraini, "Sistem Pengendali Lingkungan Pertanian Dengan Wireless Sensor Network Untuk Mengoptimalkan Budidaya Hidroponik," 2024. doi: 10.47709/digitech.v3i2.3461.

[25] F. P. Eka Putra, A. M. Ubaidillah Solichin, M. N. Wildanul Hakim, and M. T. Ramadhan, "Pemanfaatan Teknologi Wireless dan Mobile Network Berbasis 5G Untuk Pemerataan Akses Jaringan di Indonesia," *Infotek J. Inform. dan Teknol.*, vol. 8, no. 2, pp. 415–425, 2025, doi: 10.29408/jit.v8i2.30559.

[26] A. Zulfikri, F. P. E. Putra, M. A. Huda, H. Hasbullah, M. Mahendra, and M. Surur, "Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Filtering Firewall Dengan Port Blocking," 2023. doi: 10.47709/digitech.v3i2.3379.

[27] F. P. Eka Putra, F. Muslim, N. Hasanah, Holipah, R. Paradina, and R. Alim, "Analisis Komparasi Protokol Websocket dan MQTT Dalam Proses Push Notification," *J. Sistim Inf. dan Teknol.*, pp. 63–72, 2024, doi: 10.60083/jsisfotek.v5i4.325.

[28] J. Liu *et al.*, "Multi-Job Intelligent Scheduling With Cross-Device Federated Learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 34, no. 2, pp. 535–551, 2023, doi: 10.1109/TPDS.2022.3224941.

[29] Fauzan Prasetyo Eka Putra, Dea Aulia Siswoyo, M. Idris Ainul Yaqin, and Rica Oktavia, "Tinjauan Regulasi Siber dan Kebijakan Keamanan Jaringan 5G: Perspektif Nasional dan Internasional," 2025, *researchgate.net*. doi: 10.55606/jitek.v5i1.6141.

[30] S. Arifin, N. P. Dewi, . U., M. N. Arifin, and F. P. E. Putra, "Aplikasi Pengolahan Data Mahasiswa Kkn Pada Universitas Madura," *Insa. Comtech Inf. Sci. Comput. Technol. J.*, vol. 8, no. 2, p. 24, 2023, doi: 10.53712/jic.v8i2.2085.

[31] S. S. Sran, S. K. Sidhu, M. Kumar, and P. Sood, "Dynamic Route Management for Secure Data Aggregation in Duty-Cycled Mobile Sink-Based WSNs," *SN Comput. Sci.*, vol. 6, no. 3, 2025, doi: 10.1007/s42979-025-03780-1.

[32] H. A. H. Nguyen and C. H. Kim, "Efficient Bearing Fault Diagnosis for Edge Computing Using Grayscale Spectrograms and Hybrid Neural Model Compression," *IEEE Access*, vol. 13, pp. 147494–147510, 2025, doi: 10.1109/ACCESS.2025.3600678.

[33] I. Hidayatullah, M. H. Khairi, I. Maulana, and F. P. Eka Putra, "Analisis Protokol Keamanan Jaringan dalam Era Internet of Things (IoT)," *Infotek J. Inform. dan Teknol.*, vol. 8, no. 2, pp. 356–366, 2025, doi: 10.29408/jit.v8i2.30257.

[34] H. Geng and Q. Zhang, "Research on Intra-Domain Routing Protection Scheme Based on SRv6," *Comput. Eng. Appl.*, vol. 60, no. 6, pp. 293–300, 2024, doi: 10.3778/j.issn.1002-8331.2210-0463.

[35] L. Liu, A. Malmert, E. Pouyet, S. Mirri, and G. Delnevo, "Joined Spatial and Spectral Segmentation of

Hyperspectral Datasets on Historical Art Objects," *IEEE Access*, vol. 13, pp. 108266–108283, 2025, doi: 10.1109/ACCESS.2025.3579076.

[36] T. D. Cao, H. T. Nguyen, M. T. Nguyen, T. Truong-Huu, and H. L. Truong, "EADRAN: An edge marketplace for federated learning," *Futur. Gener. Comput. Syst.*, vol. 175, 2026, doi: 10.1016/j.future.2025.108046.

[37] K. N. Lal, "A lung sound recognition model to diagnoses the respiratory diseases by using transfer learning," *Multimed. Tools Appl.*, vol. 82, no. 23, pp. 36615–36631, 2023, doi: 10.1007/s11042-023-14727-0.

[38] J. A. Berrios Moya, J. Ayoade, and M. A. Uddin, "A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System," *Sensors*, vol. 25, no. 11, 2025, doi: 10.3390/s25113450.

[39] A. Rozario, E. Ahmed, and N. Mansoor, "A Robust Routing Protocol in Cognitive Unmanned Aerial Vehicular Networks," *Sensors*, vol. 24, no. 19, 2024, doi: 10.3390/s24196334.

[40] F. P. E. Putra, M. Aziz, G. Arifin, A. Rohman, A. Rizki, and A. M. Syam, "Analisis Qos & Qoe," *J. Syntax Admiration*, vol. 5, no. 1, pp. 140–145, 2024, doi: 10.46799/jsa.v5i1.973.

[41] Z. Lv, X. Li, Y. Peng, and J. Huang, "Optimized Space-Filling Curve-Driven Forward-Secure Range Query on Location-Related Data for Unmanned Aerial Vehicle Networks," *Electron.*, vol. 14, no. 10, 2025, doi: 10.3390/electronics14101978.

[42] A. Jovanović, I. B. Djordjevic, Z. H. Perić, and S. A. Vlajkov, "Circularly Symmetric Companding Quantization- Inspired Hybrid Constellation Shaping for APSK Modulation to Increase Power Efficiency in Gaussian-Noise-Limited Channel," *IEEE Access*, vol. 9, pp. 4072–4083, 2021, doi: 10.1109/ACCESS.2020.3047681.

[43] S. K. Si *et al.*, "Enhancement of the piezoelectric performance of GN nanosheets/PVDF nanocomposite film using electrostatic layer and penetrated electrode," *J. Alloys Compd.*, vol. 1001, 2024, doi: 10.1016/j.jallcom.2024.175160.

[44] G. H. Adday, S. K. Subramaniam, Z. A. Zukarnain, and N. Samian, "Investigating and Analyzing Simulation Tools of Wireless Sensor Networks: A Comprehensive Survey," *IEEE Access*, vol. 12, pp. 22938–22977, 2024, doi: 10.1109/ACCESS.2024.3362889.

[45] N. A. Saeed *et al.*, "Nonlinear vibration of quasi-zero stiffness structure with piezoelectric harvester and RL-load: intra-well and inter-well oscillation modes under 1:1 internal resonance," *Appl. Math. Mech. (English Ed.)*, vol. 46, no. 8, pp. 1451–1474, 2025, doi: 10.1007/s10483-025-3285-8.

[46] M. Khofikur R.A, F. P. Eka Putra, M. W. Ridho G, and V. Huda, "Analisis Kinerja dan Keamanan Protokol PPTP dan L2TP/IPSec VPN pada Jaringan MikroTik," *Infotek J. Inform. dan Teknol.*, vol. 8, no. 2, pp. 334–344, 2025, doi: 10.29408/jit.v8i2.30230.

[47] A. Delham Algarni, F. Algarni, S. Ullah Jan, and N. Innab, "LSP-eHS: A Lightweight and Secure Protocol for e-Healthcare System," *IEEE Access*, vol. 12, pp. 156849–156866, 2024, doi: 10.1109/ACCESS.2024.3477922.

[48] Fauzan Prasetyo Eka Putra, Debri Eko Arissandi, Achmad Rofiqi, and Moh Firman Hidayat, "Pemanfaatan Mikrotik Dalam Manajemen Bandwidth Pada Jaringan Sekolah," 2025, *researchgate.net*. doi: 10.55606/jitek.v5i1.5938.

[49] D. Fotue and H. Labiod, "Efficient Tree Aggregation and Processing Time for Wireless Sensor Networks," *Mob. Networks Appl.*, vol. 28, no. 1, pp. 160–167, 2023, doi: 10.1007/s11036-023-02088-9.

[50] A. Alzahrani, "RLKS-TMS: A Robust and Lightweight Key Agreement Scheme for Telemedicine System,"

IEEE Access, vol. 12, pp. 108233–108247, 2024, doi: 10.1109/ACCESS.2024.3422038.