JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Studi Literatur : Perkembangan Teknologi Firewall Dan Strategi Pertahanan Jaringan Pada Sistem Komputer

Cut Tarina[1*], Nazwa Ismara [2], Lili Mahara [3], Alysa[4], Nahwah Azimah[5]
[1,2,3,4,5]Teknik Informatika Universitas Malikussaleh, Indonesia
Jl. Kampus Unimal Bukit Indah, Blang Pulo, Kec. Muara Satu,Kota Lhokseumawe, Aceh 24355 email:
[1]cut.240170149@mhs.unimal.ac.id, [2]nazwaismara@gmail.com, [3]lilimahara87@gmail.com, [4]alysaa0202@gmail.com, [5]nahwaazima01@gmail.com

ABSTRACT

The rapid advancement of information technology has significantly increased dependence on digital networks, making network security a critical concern amid the growing complexity of cyber threats. Traditional security mechanisms are no longer sufficient to address modern attacks such as malware, Distributed Denial of Service (DDoS), ransomware, and application-based intrusions(Bellamkonda, 2024; Patel, 2024). *This study aims to systematically examine the development of firewall technologies from early generations to modern solutions and to analyze network defense strategies applied to mitigate contemporary cyber threats. This research employs a literature review method by analyzing scientific journals, textbooks, and international standards related to network security, firewall technologies, and defense strategies published between 2020 and 2025. The collected literature was analyzed using qualitative descriptive analysis to identify trends, characteristics, and challenges in firewall implementation. The results indicate that modern firewalls, particularly Next-Generation Firewalls (NGFW) and cloud-based firewalls, offer enhanced capabilities such as deep packet inspection, application control, and real-time threat prevention*(George & George, 2021; Patel, 2024). *However, their effectiveness largely depends on proper configuration and integration with layered security strategies, including defense in depth, Zero Trust Architecture, IDS/IPS, VPN, and SIEM*(Bellamkonda, 2024; Rose et al., n.d.). *Despite their advantages, challenges such as high implementation costs, system complexity, and performance impact remain significant considerations.*

Keywords:
Firewall, Keamanan Jaringan, Network Defense, Cybersecurity, Next-Generation Firewall.

PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah membawa perubahan signifikan dalam pengelolaan sistem jaringan komputer di berbagai sektor, seperti bisnis, pemerintahan, dan pendidikan. Ketergantungan yang tinggi terhadap layanan digital menjadikan keamanan jaringan sebagai aspek krusial yang harus dijaga secara serius. Seiring dengan meningkatnya aktivitas digital, ancaman siber juga mengalami perkembangan yang signifikan, baik dari segi jumlah maupun kompleksitas pola serangan. Berbagai insiden keamanan, seperti pencurian data, penyebaran malware, serangan *Distributed Denial of Service* (DDoS), hingga infiltrasi jaringan berbasis aplikasi, menunjukkan bahwa mekanisme pertahanan tradisional tidak lagi memadai dalam menghadapi tantangan keamanan jaringan modern.(Bellamkonda, 2024; Surana et al., 2017)

Firewall merupakan salah satu komponen utama dalam sistem keamanan jaringan yang berfungsi sebagai penyaring, pengendali, dan pengawas lalu lintas data yang masuk dan keluar dari suatu jaringan. Secara historis, teknologi firewall mengalami evolusi yang cukup signifikan, dimulai dari firewall generasi awal yang hanya melakukan penyaringan paket (*packet filtering*) berdasarkan alamat IP dan port, hingga berkembang menjadi *Next-Generation Firewall* (NGFW) yang mampu melakukan *deep packet inspection*, analisis berbasis aplikasi, serta deteksi ancaman secara real-time. Berbagai penelitian menunjukkan bahwa firewall generasi terbaru memiliki kemampuan yang lebih adaptif dalam menghadapi ancaman siber modern, seperti ransomware, phishing, dan serangan berbasis aplikasi web.(Patel, 2024)

Meskipun teknologi firewall terus berkembang, efektivitas penerapannya tidak hanya ditentukan oleh kecanggihan perangkat, tetapi juga oleh strategi pertahanan jaringan yang digunakan, termasuk konfigurasi, kebijakan keamanan, serta kemampuan sistem dalam menyesuaikan diri terhadap ancaman baru. Kesalahan konfigurasi atau penerapan strategi yang tidak tepat dapat mengurangi tingkat perlindungan yang diberikan oleh firewall, bahkan berpotensi membuka celah keamanan baru. Oleh karena itu, pemahaman yang komprehensif mengenai perkembangan teknologi firewall dan strategi pertahanan jaringan menjadi sangat penting dalam upaya meningkatkan keamanan sistem komputer.(Bellamkonda, 2024; Erwin Dwi Setiawan, Ridwansyah, 2023)(Patel, 2024; Surana et al., 2017)

Berdasarkan kondisi tersebut, diperlukan suatu kajian literatur yang membahas secara sistematis perkembangan teknologi firewall dari generasi awal hingga teknologi terkini, serta strategi pertahanan jaringan yang diterapkan untuk

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

menghadapi ancaman siber modern. Kajian ini bertujuan untuk menjawab beberapa permasalahan utama, yaitu bagaimana perkembangan teknologi firewall dari waktu ke waktu, strategi pertahanan jaringan apa saja yang digunakan dalam menghadapi ancaman siber, serta bagaimana peran firewall dalam meningkatkan keamanan jaringan komputer berdasarkan temuan-temuan dalam literatur ilmiah.

Melalui studi literatur ini, diharapkan dapat diperoleh gambaran yang menyeluruh mengenai efektivitas firewall sebagai komponen pertahanan jaringan, baik dari sisi akademis maupun praktis. Secara akademis, penelitian ini diharapkan dapat menjadi referensi ilmiah dalam bidang keamanan jaringan komputer. Secara praktis, hasil kajian ini diharapkan dapat memberikan wawasan bagi praktisi teknologi informasi dalam memilih dan menerapkan teknologi firewall yang sesuai. Selain itu, penelitian ini juga diharapkan dapat meningkatkan kesadaran masyarakat mengenai pentingnya keamanan data dan perlindungan jaringan dalam aktivitas digital sehari-hari.

KAJIAN LITERATUR

Konsep Dasar Keamanan Jaringan

Keamanan jaringan merupakan seperangkat kebijakan, praktik, serta teknologi yang dirancang untuk melindungi integritas, kerahasiaan, dan ketersediaan data serta sumber daya jaringan dari berbagai ancaman, baik yang berasal dari internal maupun eksternal. Tujuan utama dari keamanan jaringan meliputi pencegahan akses tidak sah, pendeteksian aktivitas mencurigakan atau penyusupan, serta kemampuan pemulihan sistem setelah terjadi insiden keamanan. Dalam konteks sistem komputer modern yang saling terhubung, keamanan jaringan menjadi fondasi utama dalam menjaga keberlangsungan layanan dan kepercayaan pengguna.

Konsep keamanan jaringan secara umum berlandaskan pada prinsip *CIA Triad*, yaitu *Confidentiality*, *Integrity*, dan *Availability*. *Confidentiality* (kerahasiaan) menekankan bahwa informasi hanya dapat diakses oleh pihak yang berwenang. *Integrity* (integritas) memastikan bahwa data tetap akurat dan tidak mengalami perubahan yang tidak sah selama proses penyimpanan maupun transmisi. Sementara itu, *Availability* (ketersediaan) menjamin bahwa informasi dan layanan jaringan dapat diakses saat dibutuhkan oleh pengguna yang sah. Ketiga prinsip ini hingga saat ini masih menjadi dasar dalam perancangan kebijakan keamanan, arsitektur sistem, serta pengukuran risiko keamanan informasi.(Patel, 2024; Surana et al., 2017)

Literatur juga mengidentifikasi berbagai jenis ancaman jaringan yang terus berkembang seiring dengan kemajuan teknologi. Salah satu ancaman yang paling umum adalah serangan *Distributed Denial of Service* (DDoS), yaitu upaya melumpuhkan layanan dengan membanjiri sistem target menggunakan lalu lintas berlebih sehingga layanan tidak dapat diakses. Ancaman lainnya adalah *spoofing*, yaitu pemalsuan identitas sumber, seperti alamat IP atau MAC, untuk menyamarkan pelaku serangan. Selain itu, malware yang mencakup virus, trojan, dan worm masih menjadi ancaman serius karena dapat merusak sistem atau mencuri data. Dalam beberapa tahun terakhir, ransomware muncul sebagai salah satu ancaman paling berbahaya karena mengenkripsi data korban dan menuntut tebusan, sehingga berdampak signifikan terhadap operasional organisasi.(Bellamkonda, 2024; Yusuf et al., 2020)

Firewall

Firewall merupakan komponen penting dalam keamanan jaringan yang berfungsi mengatur lalu lintas data yang masuk dan keluar dari suatu jaringan berdasarkan kebijakan keamanan yang telah ditetapkan. Fungsi utama firewall meliputi penyaringan (*filtering*), pemantauan (*monitoring*), pemblokiran lalu lintas berbahaya, serta pengendalian akses (*access control*). Firewall dapat ditempatkan pada perimeter jaringan sebagai garis pertahanan pertama, maupun pada segmen internal jaringan untuk membatasi pergerakan lateral apabila terjadi kompromi pada salah satu bagian sistem.(George & George, 2021)

Klasifikasi Firewall Berdasarkan Generasinya

Perkembangan teknologi firewall dalam literatur umumnya diklasifikasikan ke dalam beberapa generasi. Firewall generasi pertama dikenal sebagai *packet filtering firewall*, yang melakukan pemeriksaan sederhana terhadap header paket berdasarkan alamat IP dan nomor port. Meskipun efektif untuk kontrol dasar, jenis firewall ini memiliki keterbatasan dalam mendeteksi serangan pada tingkat aplikasi.(Mohammed & Shaik, 2025; Surana et al., 2017)

Firewall generasi kedua, yaitu *stateful inspection firewall*, memperkenalkan kemampuan untuk melacak status koneksi, seperti proses *handshake* pada protokol TCP, sehingga mampu memberikan konteks yang lebih baik dibandingkan penyaringan paket statis. Selanjutnya, firewall generasi ketiga atau *application layer firewall* mampu melakukan penyaringan berdasarkan aplikasi dan protokol tertentu, seperti HTTP atau SMTP, serta memeriksa muatan data pada tingkat aplikasi. (George & George, 2021; Patel, 2024)

Perkembangan signifikan terjadi pada firewall generasi keempat yang dikenal sebagai *Next-Generation Firewall* (NGFW). NGFW mengintegrasikan berbagai kemampuan lanjutan, seperti *Deep Packet Inspection* (DPI), kontrol aplikasi, identifikasi pengguna, serta integrasi dengan *Intrusion Prevention System* (IPS) dan *threat intelligence*. Firewall jenis ini dirancang untuk menghadapi ancaman siber modern, termasuk *Advanced Persistent Threat* (APT) dan

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

serangan berbasis aplikasi. Lebih lanjut, firewall generasi kelima mulai mengarah pada solusi berbasis cloud dan pemanfaatan kecerdasan buatan atau pembelajaran mesin, yang dikenal sebagai *Firewall as a Service* (FWaaS) atau firewall adaptif, sehingga lebih sesuai untuk lingkungan komputasi awan dan arsitektur jaringan terdistribusi.(Bellamkonda, 2024; Mr. Apoorva Karambelkar; Mr. Shivam Gupta; Ms. Vidhi Agarwal; Mrs. Sonia Behra, 2025)

Teknologi Firewall Modern

Firewall modern dilengkapi dengan berbagai teknologi pendukung untuk meningkatkan efektivitas perlindungan jaringan. Salah satu teknologi utama adalah *Deep Packet Inspection* (DPI), yang memungkinkan firewall untuk memeriksa muatan paket secara mendalam guna mengidentifikasi aplikasi, pola serangan, atau upaya pencurian data. Meskipun efektif, DPI menghadapi tantangan ketika lalu lintas data dienkripsi, sehingga penelitian terkini juga membahas pendekatan inspeksi yang tetap menjaga privasi.(Bellamkonda, 2024; Patel, 2024)

Integrasi *Intrusion Prevention System* (IPS) pada firewall modern memungkinkan pemblokiran aktivitas berbahaya secara real-time berdasarkan pola serangan yang telah dikenal maupun analisis heuristik. Selain itu, penggunaan *sandboxing* dan *threat intelligence* memungkinkan analisis perilaku terhadap file atau lalu lintas mencurigakan serta pemanfaatan informasi reputasi untuk mendeteksi indikator kompromi. Perkembangan lainnya adalah penerapan firewall berbasis cloud atau FWaaS yang menawarkan skalabilitas tinggi dan integrasi dengan konsep *Secure Access Service Edge* (SASE) serta *Software-Defined Wide Area Network* (SD-WAN). Firewall modern juga semakin sering diintegrasikan dalam arsitektur *Zero Trust Network Access* (ZTNA) untuk menerapkan kontrol akses berbasis konteks. (Bellamkonda, 2024)

Strategi Pertahanan Jaringan

Defense in Depth

Strategi *defense in depth* menekankan penerapan keamanan berlapis pada berbagai tingkat sistem, mulai dari perimeter jaringan, jaringan internal, endpoint, hingga aplikasi. Pendekatan ini bertujuan untuk memastikan bahwa kegagalan pada satu lapisan tidak serta-merta menyebabkan kegagalan total sistem. Dalam praktiknya, strategi ini mengombinasikan kontrol preventif, detektif, dan responsif, seperti penggunaan firewall perimeter, segmentasi jaringan internal, perlindungan endpoint, serta sistem pemantauan terpusat seperti SIEM.(Bellamkonda, 2024; Patel, 2024)

Zero Trust Architecture

Zero Trust Architecture mengusung prinsip "*never trust, always verify*", yang menekankan bahwa setiap permintaan akses harus melalui proses autentikasi dan otorisasi secara berkelanjutan, tanpa mengandalkan kepercayaan implisit berdasarkan lokasi jaringan. Pendekatan ini menerapkan prinsip *least privilege* dan *micro-segmentation* untuk membatasi pergerakan lateral dalam jaringan. Literatur dan standar seperti NIST SP 800-207 banyak dijadikan acuan dalam perancangan dan implementasi arsitektur Zero Trust.(Rose et al., n.d.)

Intrusion Detection and Prevention System (IDS/IPS)

IDS dan IPS merupakan komponen penting dalam strategi pertahanan jaringan. IDS berfungsi mendeteksi aktivitas mencurigakan dan memberikan peringatan, sedangkan IPS mampu mengambil tindakan otomatis untuk memblokir lalu lintas berbahaya. Metode deteksi dapat berbasis tanda tangan (*signature-based*) maupun anomali (*anomaly-based*). Deteksi berbasis tanda tangan efektif untuk serangan yang telah dikenal, sementara deteksi berbasis anomali lebih adaptif terhadap ancaman baru, meskipun berpotensi menghasilkan *false positive*. Oleh karena itu, banyak penelitian merekomendasikan pendekatan hibrida yang menggabungkan kedua metode tersebut dengan dukungan pembelajaran mesin.(Patel, 2024; Surana et al., 2017)

Virtual Private Network (VPN)

Virtual Private Network (VPN) menyediakan mekanisme enkripsi dan *tunneling* untuk mengamankan komunikasi jarak jauh, seperti melalui protokol IPsec, OpenVPN, atau WireGuard. Meskipun VPN mampu melindungi saluran komunikasi, model VPN tradisional cenderung memberikan akses jaringan yang luas setelah autentikasi, sehingga kurang sejalan dengan prinsip Zero Trust. Hal ini mendorong munculnya konsep integrasi VPN dengan ZTNA atau penerapan *Zero Trust VPN*. Kinerja VPN dipengaruhi oleh protokol yang digunakan, metode enkripsi, dan beban jaringan, sehingga teknologi yang lebih modern dirancang untuk mengurangi latensi dan overhead.(Bellamkonda, 2024)

Security Information and Event Management (SIEM)

SIEM merupakan sistem yang berfungsi mengumpulkan, mengkorelasikan, dan menganalisis log dari berbagai sumber keamanan, seperti firewall, IDS/IPS, dan endpoint. Dengan kemampuan analitik yang terpusat, SIEM mendukung deteksi insiden, pelaporan keamanan, serta respons insiden yang lebih cepat. Perkembangan SIEM juga

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

mengarah pada integrasi dengan *Security Orchestration, Automation, and Response* (SOAR) serta pemanfaatan analitik berbasis pembelajaran mesin. Dalam konteks organisasi menengah dan kecil, solusi SIEM *open-source* banyak dibahas dalam literatur sebagai alternatif yang lebih ekonomis namun tetap efektif.(Bellamkonda, 2024; Fitrian et al., 2025)

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kepustakaan (*library research*). Metode ini dilakukan dengan mengumpulkan, menelaah, dan menganalisis berbagai sumber ilmiah yang relevan dengan topik keamanan jaringan, perkembangan teknologi firewall, serta strategi pertahanan jaringan modern. Pendekatan penelitian kepustakaan dipilih karena penelitian ini berfokus pada kajian konseptual dan analisis terhadap teori, hasil penelitian terdahulu, serta dokumen teknis yang berkaitan dengan sistem keamanan jaringan komputer, tanpa melibatkan pengumpulan data empiris secara langsung di lapangan.

Sumber Data

Sumber data dalam penelitian ini berasal dari berbagai literatur ilmiah yang kredibel dan relevan, meliputi:

1. Jurnal ilmiah nasional dan internasional yang membahas keamanan jaringan, firewall, dan strategi pertahanan jaringan.
2. Buku teks dan dokumen teknis yang mengulas konsep dasar keamanan jaringan dan implementasi teknologi firewall.
3. Standar dan pedoman internasional, seperti NIST SP 800-207 yang membahas *Zero Trust Architecture*.
4. Artikel dan publikasi ilmiah lainnya yang membahas perkembangan teknologi firewall, mulai dari firewall generasi awal hingga firewall generasi terbaru.

Literatur yang digunakan dibatasi pada publikasi dalam rentang waktu lima tahun terakhir (2020–2025) guna memastikan relevansi pembahasan terhadap perkembangan ancaman siber dan teknologi keamanan jaringan terkini.

Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui beberapa tahapan sistematis. Tahap awal dimulai dengan identifikasi topik dan ruang lingkup penelitian berdasarkan rumusan masalah yang telah disusun pada bagian pendahuluan. Selanjutnya, dilakukan penelusuran literatur menggunakan kata kunci yang relevan, seperti *firewall*, *network security*, *Next-Generation Firewall*, *DDoS mitigation*, *Deep Packet Inspection*, *Zero Trust*, dan *Security Information and Event Management* (SIEM).

Literatur yang diperoleh kemudian diseleksi berdasarkan beberapa kriteria, yaitu kesesuaian dengan topik penelitian, tahun publikasi, serta kredibilitas sumber, seperti jurnal terindeks, standar internasional, dan buku resmi. Tahap akhir dari pengumpulan data adalah pencatatan dan ekstraksi informasi penting yang berkaitan dengan definisi, konsep, perkembangan teknologi firewall, serta strategi pertahanan jaringan komputer.

Teknik Analisis Data

Teknik analisis data yang digunakan dalam penelitian ini adalah analisis deskriptif kualitatif. Analisis dilakukan dengan mengelompokkan literatur berdasarkan tema-tema utama, seperti keamanan jaringan, ancaman jaringan, teknologi firewall, IDS/IPS, VPN, *Zero Trust Architecture*, dan *defense in depth*. Selanjutnya, dilakukan perbandingan perkembangan teknologi firewall dari generasi awal hingga *Next-Generation Firewall* berdasarkan temuan dalam literatur.

Hasil analisis kemudian disintesis untuk mengidentifikasi pola, kecenderungan, serta peran firewall dalam mendukung strategi pertahanan jaringan modern. Proses analisis ini bertujuan untuk menghasilkan pemahaman yang komprehensif dan terstruktur guna menjawab rumusan masalah penelitian.

Prosedur Penelitian

Prosedur penelitian dilaksanakan melalui beberapa tahapan. Tahap pertama adalah penetapan masalah dan ruang lingkup penelitian berdasarkan latar belakang dan tujuan penelitian. Tahap kedua meliputi pengumpulan literatur dari jurnal ilmiah, buku, serta standar internasional yang relevan. Tahap selanjutnya adalah seleksi dan evaluasi kualitas literatur untuk memastikan validitas dan relevansi sumber yang digunakan.

Tahap analisis dilakukan untuk mengkaji perkembangan teknologi firewall, strategi pertahanan jaringan yang diterapkan, serta peran firewall dalam meningkatkan keamanan jaringan komputer. Tahap akhir adalah penyusunan pembahasan dan penarikan kesimpulan berdasarkan hasil kajian literatur yang telah dianalisis secara sistematis.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil analisis berdasarkan kajian literatur yang telah dikumpulkan dan dianalisis secara sistematis pada bab sebelumnya, serta membahas temuan-temuan penelitian terdahulu dalam konteks perkembangan teknologi firewall dan strategi pertahanan jaringan pada sistem komputer. Pembahasan difokuskan pada sintesis hasil penelitian untuk menjawab rumusan masalah penelitian, sehingga tidak hanya bersifat deskriptif, tetapi juga analitis dan integratif.

Perkembangan Teknologi Firewall

Hasil kajian literatur menunjukkan bahwa teknologi firewall mengalami perkembangan yang signifikan seiring dengan meningkatnya kompleksitas ancaman siber. Firewall generasi awal yang mengandalkan *packet filtering* hanya melakukan penyaringan lalu lintas berdasarkan alamat IP dan nomor port. Pendekatan ini efektif untuk pengendalian lalu lintas dasar dan memiliki performa yang tinggi, namun sangat terbatas dalam mendeteksi serangan yang bekerja pada tingkat aplikasi.

Perkembangan berikutnya menghadirkan *stateful inspection firewall* yang mampu melacak status koneksi jaringan. Dengan memahami konteks koneksi, firewall jenis ini meningkatkan akurasi penyaringan dibandingkan firewall tradisional. Selanjutnya, *application layer firewall* mulai diterapkan untuk menyaring lalu lintas berdasarkan aplikasi dan protokol tertentu, sehingga mampu mengurangi risiko serangan berbasis aplikasi, meskipun masih menghadapi tantangan pada aspek performa dan skalabilitas.

Tonggak utama dalam evolusi firewall ditandai dengan kemunculan *Next-Generation Firewall* (NGFW). Firewall generasi ini mengintegrasikan berbagai fitur lanjutan, seperti *Deep Packet Inspection* (DPI), kontrol aplikasi, identitas pengguna, serta *Intrusion Prevention System* (IPS). Berbagai studi literatur, termasuk penelitian pada jurnal nasional bidang komputasi dan teknologi informasi, menunjukkan bahwa NGFW secara signifikan lebih efektif dalam menyaring lalu lintas berbahaya dan memblokir ancaman lanjutan, seperti *Advanced Persistent Threat* (APT), ransomware, dan serangan berbasis aplikasi web, dibandingkan firewall generasi sebelumnya.

Selain NGFW, literatur juga menunjukkan perkembangan menuju firewall berbasis *Software-Defined Networking* (SDN) dan pemanfaatan kecerdasan buatan. Firewall jenis ini mengadopsi analisis perilaku dan pendekatan adaptif untuk meningkatkan kemampuan deteksi ancaman, terutama terhadap serangan yang bersifat dinamis dan belum memiliki pola tetap.

Karakteristik dan Efektivitas Firewall Generasi Baru (NGFW)

Hasil analisis literatur menunjukkan bahwa NGFW tidak hanya memperluas fungsi firewall tradisional, tetapi juga meningkatkan visibilitas dan kontrol terhadap lalu lintas jaringan. Dengan dukungan DPI, NGFW mampu memeriksa muatan paket hingga lapisan aplikasi, sehingga dapat membedakan lalu lintas yang sah dan berbahaya secara lebih akurat. Integrasi IPS memungkinkan firewall tidak hanya mendeteksi, tetapi juga mencegah serangan secara real-time.

Selain itu, NGFW mendukung penerapan kebijakan keamanan berbasis identitas pengguna dan aplikasi, bukan hanya berdasarkan alamat IP atau port. Integrasi *threat intelligence* dari berbagai sumber global juga memungkinkan firewall merespons ancaman baru secara lebih cepat. Hasil penelitian pada beberapa studi kasus di lingkungan organisasi menunjukkan bahwa konfigurasi NGFW yang tepat, disertai fitur seperti *web filtering* dan kontrol aplikasi, mampu membatasi akses berbahaya serta meningkatkan visibilitas terhadap lalu lintas internal dan eksternal jaringan.

Meskipun demikian, efektivitas NGFW sangat dipengaruhi oleh kebijakan dan konfigurasi yang diterapkan. Literatur menekankan bahwa kesalahan konfigurasi masih menjadi salah satu penyebab utama terjadinya celah keamanan, sehingga pengelolaan firewall secara berkelanjutan merupakan faktor penting dalam menjaga keamanan jaringan. (Bellamkonda, 2024; Patel, 2024)

Firewall Berbasis Cloud dan Kecerdasan Buatan

Perkembangan teknologi keamanan jaringan juga mengarah pada penerapan firewall berbasis cloud atau *Firewall as a Service* (FWaaS). Model ini memindahkan fungsi firewall ke platform cloud, sehingga kebijakan keamanan dapat dikelola secara terpusat dan diterapkan secara konsisten pada pengguna serta aplikasi yang tersebar di berbagai lokasi. Pendekatan ini dinilai lebih fleksibel dan skalabel dibandingkan penggunaan perangkat firewall fisik, terutama pada lingkungan komputasi awan dan organisasi dengan infrastruktur terdistribusi.

Selain itu, integrasi kecerdasan buatan dan *machine learning* dalam sistem firewall menjadi fokus penelitian terkini. Beberapa studi menunjukkan bahwa penggunaan algoritma pembelajaran mesin, seperti *Random Forest*, pada arsitektur SDN mampu meningkatkan akurasi deteksi serangan, termasuk serangan DDoS, serta mengurangi tingkat *false positive* dibandingkan pendekatan berbasis aturan statis. Temuan ini menunjukkan bahwa firewall adaptif berbasis AI memiliki potensi besar dalam menghadapi ancaman siber yang terus berkembang. (Bellamkonda, 2024)

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

Strategi Pertahanan Jaringan dalam Menghadapi Ancaman Siber

Hasil kajian literatur menunjukkan bahwa pertahanan jaringan yang efektif tidak dapat bergantung pada satu mekanisme keamanan saja. Pendekatan *defense in depth* menjadi strategi yang paling banyak direkomendasikan, karena menerapkan lapisan keamanan berlapis mulai dari firewall, IDS/IPS, segmentasi jaringan, hingga perlindungan endpoint dan sistem pemantauan terpusat.

Integrasi firewall dengan IDS dan IPS terbukti meningkatkan kemampuan deteksi dan pencegahan serangan. Firewall berperan sebagai penyaring lalu lintas utama, sementara IDS/IPS menganalisis pola serangan yang lebih kompleks dan mampu melakukan respons aktif terhadap lalu lintas berbahaya. Selain itu, segmentasi jaringan diterapkan untuk membatasi pergerakan lateral ancaman sehingga kompromi pada satu segmen tidak langsung berdampak pada keseluruhan sistem.

Pendekatan *Zero Trust Architecture* juga semakin banyak diadopsi dalam strategi pertahanan jaringan modern. Prinsip "*never trust, always verify*" diterapkan untuk memastikan bahwa setiap permintaan akses selalu melalui proses autentikasi dan otorisasi. Literatur menunjukkan bahwa penerapan Zero Trust mampu mengurangi risiko serangan seperti *man-in-the-middle* dan DDoS, meskipun dalam beberapa kasus dapat menimbulkan penurunan performa jaringan yang perlu dioptimalkan.(Bellamkonda, 2024; Rose et al., n.d.)

Penggunaan Virtual Private Network (VPN) masih relevan untuk mengamankan komunikasi jarak jauh, namun model VPN tradisional memiliki keterbatasan dalam mendukung prinsip Zero Trust. Oleh karena itu, integrasi VPN dengan *Zero Trust Network Access* (ZTNA) menjadi solusi yang semakin banyak dibahas. Di sisi lain, pemanfaatan *Security Information and Event Management* (SIEM) memungkinkan pengumpulan dan korelasi log dari berbagai sumber keamanan untuk mendukung deteksi dan respons insiden secara real-time.

Analisis Integratif dan Tantangan Implementasi

Sintesis dari berbagai literatur menunjukkan bahwa firewall modern, khususnya NGFW dan firewall berbasis cloud, tidak lagi berfungsi sebagai perangkat tunggal, melainkan sebagai bagian integral dari arsitektur keamanan berlapis. Kombinasi firewall, IDS/IPS, segmentasi jaringan, Zero Trust, dan SIEM membentuk sistem pertahanan yang saling melengkapi dalam menghadapi ancaman siber modern.(Bellamkonda, 2024; Erwin Dwi Setiawan, Ridwansyah, 2023)

Namun demikian, literatur juga mengidentifikasi beberapa tantangan dalam implementasi strategi pertahanan jaringan tersebut. Tantangan utama meliputi tingginya biaya investasi dan lisensi teknologi keamanan lanjutan, kompleksitas integrasi antar komponen sistem, kebutuhan sumber daya manusia yang memiliki keahlian khusus di bidang keamanan jaringan, serta potensi penurunan performa akibat penerapan fitur keamanan yang kompleks seperti DPI dan analisis berbasis kecerdasan buatan. Oleh karena itu, perencanaan yang matang dan pengelolaan yang berkelanjutan menjadi kunci dalam mengoptimalkan penerapan teknologi firewall dan strategi pertahanan jaringan.

KESIMPULAN

Berdasarkan hasil kajian literatur dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa perkembangan teknologi firewall menunjukkan evolusi yang signifikan seiring dengan meningkatnya kompleksitas ancaman siber pada sistem komputer. Firewall tidak lagi berfungsi sebatas penyaring lalu lintas jaringan secara sederhana, melainkan telah berkembang menjadi sistem keamanan yang mampu melakukan inspeksi mendalam, analisis perilaku, serta pencegahan ancaman secara real-time melalui integrasi dengan teknologi lain seperti Intrusion Prevention System, threat intelligence, dan kecerdasan buatan.

Hasil kajian menunjukkan bahwa firewall generasi baru, khususnya Next-Generation Firewall (NGFW), memiliki efektivitas yang lebih tinggi dibandingkan firewall generasi sebelumnya dalam menghadapi ancaman siber modern, seperti serangan berbasis aplikasi, ransomware, dan Advanced Persistent Threat. Kemampuan NGFW dalam menerapkan kontrol berbasis aplikasi dan identitas pengguna menjadikannya komponen penting dalam arsitektur keamanan jaringan modern. Selain itu, perkembangan firewall berbasis cloud dan Firewall as a Service (FWaaS) menawarkan fleksibilitas dan skalabilitas yang lebih baik, terutama pada lingkungan jaringan terdistribusi dan komputasi awan.

Kajian ini juga menunjukkan bahwa efektivitas firewall sangat bergantung pada strategi pertahanan jaringan yang diterapkan. Pendekatan defense in depth dan Zero Trust Architecture menjadi strategi yang paling banyak direkomendasikan dalam literatur karena mampu memberikan perlindungan berlapis dan membatasi pergerakan lateral ancaman. Integrasi firewall dengan IDS/IPS, segmentasi jaringan, VPN berbasis Zero Trust, serta sistem pemantauan terpusat seperti Security Information and Event Management (SIEM) terbukti dapat meningkatkan ketahanan jaringan terhadap berbagai jenis serangan siber.

Meskipun demikian, literatur juga mengidentifikasi sejumlah tantangan dalam penerapan teknologi firewall dan strategi pertahanan jaringan, antara lain tingginya biaya implementasi, kompleksitas integrasi sistem, kebutuhan sumber daya manusia yang kompeten, serta potensi penurunan performa jaringan akibat penerapan fitur keamanan yang

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

kompleks. Oleh karena itu, perencanaan yang matang, konfigurasi yang tepat, dan pengelolaan keamanan jaringan secara berkelanjutan menjadi faktor kunci dalam mengoptimalkan penerapan firewall.

Berdasarkan hasil kajian ini, dapat disimpulkan bahwa pemahaman yang komprehensif mengenai perkembangan teknologi firewall dan strategi pertahanan jaringan merupakan hal yang sangat penting dalam merancang sistem keamanan jaringan yang adaptif, efektif, dan berkelanjutan. Penelitian selanjutnya disarankan untuk mengombinasikan kajian literatur dengan studi empiris atau pengujian langsung pada lingkungan jaringan tertentu guna memperoleh gambaran yang lebih mendalam mengenai efektivitas implementasi firewall dan strategi pertahanan jaringan dalam kondisi nyata.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan dalam penyusunan artikel ini. Ucapan terima kasih disampaikan kepada tim penulis yang telah berkontribusi dalam proses diskusi, pengumpulan literatur, serta penyempurnaan naskah. Penulis juga mengapresiasi para peneliti dan penulis sebelumnya yang karya ilmiahnya menjadi sumber referensi utama dalam kajian ini. Selain itu, penulis mengucapkan terima kasih kepada institusi pendidikan tempat penulis bernaung yang telah menyediakan akses terhadap sumber pustaka dan fasilitas pendukung penelitian. Penelitian ini tidak menerima pendanaan khusus dari lembaga pendanaan publik, komersial, maupun nirlaba.

REFERENSI

Bellamkonda, S. (2024). Next-Gen Firewalls and Network Security : Enhancing Defense through Advanced Threat Mitigation Techniques. 10(6), 692–702.

Erwin Dwi Setiawan, Ridwansyah, M. R. (2023). PERANCANGAN KEAMANAN JARINGAN NEXT-GENERATION FIREWALL MENGGUNAKAN ROUTER FORTINET PADA PT. ALODOKTER TEKNOLOGI SOLUSI. 9(1), 34–39.

Fitrian, H. P., Noorjamil, B. F., Rahmawati, F., & Rachman, S. A. (2025). Analisis Efektivitas Firewall dalam Memfilter dan Melindungi Lalu Lintas Jaringan. 8(1), 95–102.

George, A. S., & George, A. S. H. (2021). A Brief Study on The Evolution of Next Generation Firewall and Web Application Firewall. 10(5), 31–37. https://doi.org/10.17148/IJARCCE.2021.10504

Mohammed, K., & Shaik, N. (2025). Next-Generation Firewalls : Beyond Traditional Perimeter Defense. 7(4), 1–6.

Mr. Apoorva Karambelkar; Mr. Shivam Gupta; Ms. Vidhi Agarwal; Mrs. Sonia Behra. (2025). Next Generation Firewall using IPS & IDS. April.

Patel, U. (2024). THE ROLE OF NEXT-GENERATION FIREWALLS IN MODERN NETWORK SECURITY : A COMPREHENSIVE ANALYSIS. 15(4), 135–154.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (n.d.). Zero Trust Architecture NIST Special Publication 800-207.

Surana, J., Singh, K., Bairagi, N., Mehto, N., & Jaiswal, N. (2017). Survey on Next Generation Firewall. 5(2), 984–988.

Yusuf, M. L., Karsono, K., & Budhisantosa, N. (2020). ANALISIS PERFORMANCE NEXT GENERATION FIREWALL DAN MIKROTIK RB1100 SEBAGAI FIREWALL UNTUK KEAMANAN JARINGAN. 5, 15–30.