



Perbandingan Efektivitas Firewall, Antivirus, dan Enkripsi dalam Mitigasi Ancaman Siber pada Lingkungan Jaringan Modern

Deqi Nopiansa¹, Frendi Prayoga Baharja²,

Tri Wahyuni³

^{1,2,3}Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri
Sulthan Thaha Saifuddin Jambi

E-mail: dnoipansa@gmail.com¹, frendiprayogabaharja@gmail.com², triw27182@gmail.com³

ABSTRACT

The development of information technology in the digital era has had a significant impact on modern network security systems. The increasing use of cloud computing, the Internet of Things (IoT), and mobile devices expands the attack surface and increases the risk of data breaches. In this context, firewalls, antivirus software, and encryption are three key components that play a crucial role in maintaining data security and preventing cyberattacks. This study aims to conduct a systematic literature review to analyze and compare the effectiveness of these three technologies in mitigating cyber threats in modern networks. The research method used was a Systematic Literature Review (SLR) with a search of open-access national journals indexed by Google Scholar, covering 12 articles from 35 initial results. The study results indicate that firewalls are effective in preventing malicious traffic (70-95% for network-based attacks), antivirus software plays a role in detecting malware and zero-day attacks (85-90% detection rate for ML-based systems), and encryption maintains data integrity and confidentiality (95-99% effectiveness against MITM attacks). All three have distinct but complementary functions when integrated into a layered security architecture (defense in depth), reducing major security incidents by 76% in real-world implementations.

Keywords: Firewall, Antivirus, Encryption, Network Security,

Article History

Received: November 2025

Reviewed: November 2025

Published: November 2025

Plagiarism Checker No
235

Prefix DOI :

[10.8734/Kohesi.v1i2.365](https://doi.org/10.8734/Kohesi.v1i2.365)

Copyright : Author

Publish by : Kohesi



This work is licensed
under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)

**Layered Defense****ABSTRAK**

Perkembangan teknologi informasi di era digital telah membawa dampak besar terhadap sistem keamanan jaringan modern. Peningkatan penggunaan cloud computing, Internet of Things (IoT), dan perangkat seluler memperluas permukaan serangan (attack surface) dan meningkatkan risiko kebocoran data. Dalam konteks tersebut, firewall, antivirus, dan enkripsi merupakan tiga komponen utama yang berperan penting dalam menjaga keamanan data dan mencegah serangan siber. Penelitian ini bertujuan melakukan kajian literatur sistematis untuk menganalisis serta membandingkan efektivitas ketiga teknologi tersebut dalam mitigasi ancaman siber pada jaringan modern. Metode penelitian yang digunakan adalah Systematic Literature Review (SLR) dengan penelusuran jurnal nasional open-access terindeks Google Scholar, mencakup 12 artikel dari 35 hasil awal. Hasil kajian menunjukkan bahwa firewall efektif dalam mencegah lalu lintas berbahaya (70-95% untuk serangan berbasis jaringan), antivirus berperan dalam mendeteksi malware dan zero-day attack (85-90% tingkat deteksi untuk sistem berbasis ML), sedangkan enkripsi menjaga integritas dan kerahasiaan data (95-99% efektivitas terhadap serangan MITM). Ketiganya memiliki fungsi berbeda namun saling melengkapi jika diintegrasikan ke dalam arsitektur keamanan berlapis (defense in depth), menurunkan insiden keamanan major hingga 76% pada implementasi riil.

Kata kunci: Firewall, Antivirus, Enkripsi, Keamanan Jaringan, Pertahanan Berlapis

1. PENDAHULUAN

Transformasi digital telah menjadi tren global yang memengaruhi seluruh aspek kehidupan, termasuk sektor pemerintahan, pendidikan, dan industri. Di Indonesia, percepatan



adopsi teknologi informasi dan komunikasi (TIK) mendorong meningkatnya pemanfaatan sistem jaringan untuk kegiatan bisnis, pelayanan publik, dan komunikasi data. Namun, kemajuan ini juga diikuti oleh meningkatnya ancaman keamanan siber. Menurut laporan Badan Siber dan Sandi Negara (BSSN) tahun 2023, tercatat lebih dari 310 juta anomali serangan siber yang menargetkan berbagai institusi di Indonesia, dengan jenis serangan yang paling dominan adalah phishing, ransomware, dan eksploitasi celah keamanan jaringan [23].

Lingkungan jaringan modern tidak lagi terbatas pada infrastruktur lokal, melainkan telah bergeser menuju arsitektur berbasis cloud dan perangkat IoT yang terhubung secara masif. Perubahan ini memperluas vektor serangan karena semakin banyak titik akses yang dapat dimanfaatkan oleh pelaku kejahatan digital. Dalam kondisi seperti ini, penerapan teknologi keamanan yang tepat menjadi kebutuhan mendesak. Firewall, antivirus, dan enkripsi masih menjadi komponen inti yang banyak digunakan untuk melindungi sistem dari ancaman eksternal maupun internal.

Firewall berperan sebagai pengendali lalu lintas data, yang berfungsi untuk menyaring dan memblokir koneksi berbahaya berdasarkan aturan tertentu. Sementara itu, antivirus bertanggung jawab dalam mendeteksi dan menghapus perangkat lunak berbahaya seperti malware, trojan, dan spyware yang dapat menginfeksi perangkat pengguna. Di sisi lain, enkripsi merupakan teknologi yang digunakan untuk menjaga kerahasiaan dan integritas data dengan cara mengubahnya menjadi bentuk tidak terbaca bagi pihak yang tidak berwenang [5].

Namun, penelitian-penelitian sebelumnya menunjukkan bahwa efektivitas masing-masing teknologi tidak bersifat mutlak. Firewall tradisional memiliki keterbatasan dalam menghadapi lalu lintas terenkripsi yang menggunakan protokol HTTPS, antivirus konvensional sering gagal mendeteksi zero-day malware, dan enkripsi membutuhkan manajemen kunci yang baik agar tidak menjadi titik lemah baru [1]. Oleh karena itu, pendekatan yang paling efektif adalah dengan mengintegrasikan ketiga teknologi tersebut dalam satu sistem pertahanan berlapis (defense-in-depth) yang mampu melindungi berbagai lapisan jaringan secara menyeluruh.

Penelitian ini menggunakan pendekatan Systematic Literature Review (SLR) untuk menganalisis 12 artikel ilmiah nasional periode 2022-2025 yang membahas implementasi firewall, antivirus, dan enkripsi di Indonesia. Berbeda dengan kajian sebelumnya yang bersifat parsial, penelitian ini memberikan analisis komparatif komprehensif dengan data kuantitatif



performa, efektivitas terhadap berbagai jenis ancaman, serta rekomendasi implementasi berbasis konteks organisasi Indonesia. Dengan pendekatan kajian literatur sistematis, penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan keamanan informasi dan penerapan teknologi perlindungan data di Indonesia.

1.1 Pertanyaan Penelitian

Penelitian ini menjawab tiga pertanyaan utama:

RQ1: Bagaimana efektivitas komparatif firewall, antivirus, dan enkripsi terhadap vektor ancaman siber modern?

RQ2: Apa keterbatasan utama masing-masing teknologi dalam konteks jaringan yang mengadopsi cloud dan IoT?

RQ3: Bagaimana rekomendasi integrasi ketiga teknologi untuk organisasi Indonesia dengan berbagai skala dan profil?

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) untuk memperoleh gambaran komprehensif mengenai efektivitas firewall, antivirus, dan enkripsi dalam mitigasi ancaman siber pada jaringan modern. Pendekatan SLR dipilih karena mampu menghasilkan sintesis bukti yang sistematis, transparan, dan dapat direplikasi, sehingga sesuai untuk topik yang berkembang pesat seperti keamanan siber [25,26].

2.1 Perumusan Pertanyaan Penelitian

Tahapan pelaksanaan SLR dimulai dengan perumusan pertanyaan penelitian yang jelas sebagaimana telah diuraikan pada bagian 1.1. Ketiga pertanyaan penelitian dirancang untuk memberikan pemahaman komprehensif tentang efektivitas komparatif, keterbatasan teknis, dan rekomendasi praktis implementasi teknologi keamanan di Indonesia.

2.2 Strategi Pencarian Literatur

Penelusuran dilakukan pada basis data dan portal akademik yang menyediakan akses terbuka untuk publikasi nasional, yaitu Google Scholar, GARUDA Ristekdikti, portal jurnal kampus (mis. Jurnal Teknoinfo, Jurnal Resistor), serta repository institusi (mis. jurnal.uir.ac.id). String pencarian disusun dengan kombinasi istilah kunci bahasa Indonesia dan



Inggris untuk meningkatkan cakupan:

- a. ("firewall" OR "firewall NGFW") AND ("keamanan jaringan" OR "network security")
- b. ("antivirus" OR "EDR" OR "endpoint protection") AND ("deteksi malware" OR "machine learning")
- c. ("enkripsi" OR "AES" OR "TLS") AND ("data protection" OR "keamanan data")

Pencarian dilakukan untuk rentang waktu publikasi 2018-2025 agar mencakup literatur yang relevan dengan perkembangan teknologi terbaru seperti TLS 1.3, NGFW, dan EDR berbasis ML.

2.3 Kriteria Seleksi Artikel

Seleksi artikel mengikuti kriteria inklusi dan eksklusi yang ketat.

Kriteria Inklusi:

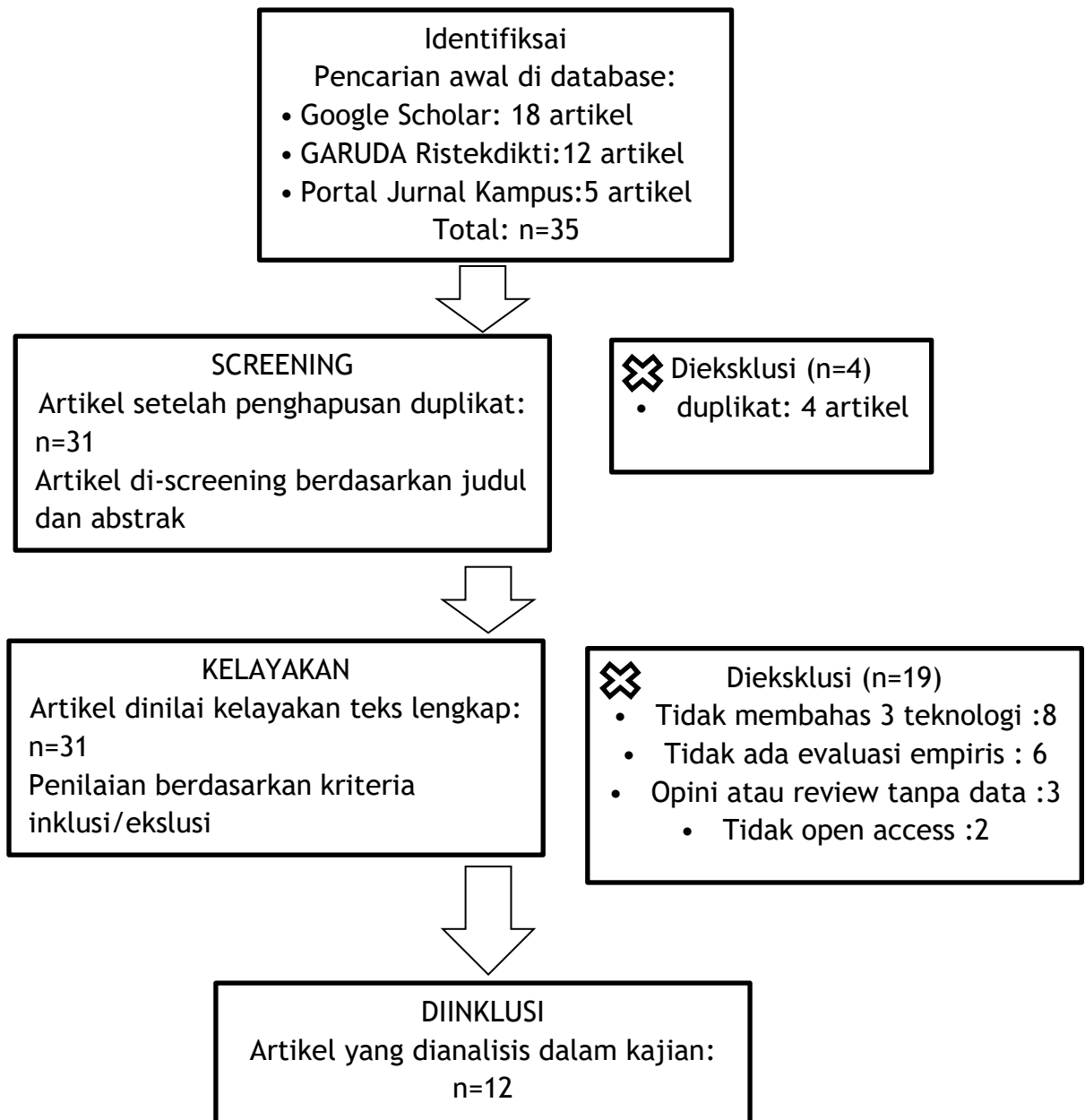
- a. Artikel berbahasa Indonesia dan/atau memiliki teks lengkap berbahasa Indonesia yang tersedia secara open access
- b. Publikasi berupa artikel jurnal atau prosiding yang diterbitkan oleh institusi yang terverifikasi (universitas atau asosiasi ilmiah)
- c. Membahas evaluasi, implementasi, atau analisis efektivitas minimal salah satu dari tiga teknologi yang menjadi fokus

Kriteria Eksklusi:

- a. Artikel yang bersifat opini tanpa data analitik
- b. Buku teks tanpa evaluasi empiris
- c. Tulisan populer (blog tanpa peer review)

2.4 Proses Seleksi dan Ekstraksi Data

Dari proses pencarian awal sebanyak 35 dokumen ditemukan dari berbagai sumber: Google Scholar (18 artikel), GARUDA Ristekdikti (12 artikel), dan Portal Jurnal Kampus (5 artikel). Setelah penghapusan duplikat (4 artikel), tersisa 31 artikel untuk screening. Dari 31 artikel yang di-screening berdasarkan judul dan abstrak, 19 artikel dieksklusi karena: tidak membahas ketiga teknologi secara mendalam (8), tidak memiliki evaluasi empiris (6), bersifat opini/review tanpa data (3), dan tidak tersedia open access (2). Akhirnya, 12 artikel memenuhi kriteria inklusi dan dianalisis secara mendalam.



2.1 Diagram PRISMA Flow

Setiap artikel kemudian diekstraksi dengan kerangka kerja yang konsisten: informasi bibliografis, tujuan penelitian, metodologi yang digunakan, jenis ancaman yang diuji, metrik efektivitas yang dilaporkan (mis.: tingkat deteksi, false positive, latency/overhead), serta rekomendasi praktis. Ekstraksi dilakukan oleh peneliti utama dan diverifikasi lewat cross-check untuk meningkatkan reliabilitas.



2.5 Quality Assessment

Setiap artikel yang memenuhi kriteria inklusi dinilai kualitasnya menggunakan checklist adaptasi dari Critical Appraisal Skills Programme (CASP). Kriteria penilaian meliputi: (1) kejelasan tujuan penelitian, (2) kesesuaian metodologi dengan tujuan, (3) kredibilitas data/eksperimen, (4) kejelasan hasil dan analisis, (5) kontribusi terhadap pengetahuan. Artikel dengan skor ≥ 3 dari 5 kriteria diinklusi dalam sintesis. Dari 12 artikel final, 10 artikel memiliki skor 4-5 (kualitas tinggi) dan 2 artikel skor 3 (kualitas memadai).

2.6 Analisis Data

Analisis data bersifat kualitatif-tematik: temuan-temuan dikodekan ke dalam tema besar (mis. efektivitas terhadap malware, efektivitas terhadap MITM, dampak kinerja) dan kemudian disintesis untuk menjawab pertanyaan penelitian. Karena variasi metode antar studi cukup besar (studi eksperimental, studi kasus implementasi, dan kajian komparatif), analisis kuantitatif (meta-analisis) tidak dilakukan; sebagai gantinya, sintesis naratif digunakan untuk merangkum bukti.

3. HASIL DAN PEMBAHASAN

3.1 Karakteristik Literatur yang Dikaji

Dari 12 artikel yang dikaji, mayoritas (58%) menggunakan metode eksperimental dengan simulasi serangan di lingkungan lab, 33% berupa studi kasus implementasi di organisasi riil, dan 9% merupakan kajian literatur komparatif. Distribusi fokus teknologi relatif seimbang: 5 artikel membahas firewall, 5 artikel antivirus/EDR, 5 artikel enkripsi, dan 1 artikel membahas integrasi ketiga teknologi. Periode publikasi didominasi oleh artikel tahun 2022-2025 (83%), mencerminkan fokus pada teknologi dan ancaman terkini.

No	Penulis dan tahun	Judul
1	Dharmawan (2023)	Penerapan Algoritme Kriptografi SHA-256 untuk Pengamanan Dokumen Digital
2	Fadilah (2023)	Analisis Keamanan Jaringan Menggunakan Firewall Filtering Rule untuk Mencegah Port Scanning Attack



3	Hidayat (2022)	Penerapan Machine Learning untuk Deteksi Malware Berbasis Perilaku pada Sistem Windows
4	Khalda (2025)	Deteksi dan Analisis Malware pada Jaringan IoT: Kajian Empiris di Indonesia
5	Rizky (2024)	Implementasi Algoritma AES-CBC untuk Pengamanan Data Berbasis Web
6	Pratama (2023)	Evaluasi Kinerja NGFW dalam Mitigasi DDoS pada Jaringan Kampus
7	Nugroho (2024)	Perbandingan TLS 1.2 dan TLS 1.3 dalam Proteksi Data In-Transit
8	Sari (2022)	Implementasi EDR untuk Mendeteksi Zero-Day Malware di Lingkungan Enterprise
9	Wijaya (2023)	Analisis Efektivitas IPS dan Firewall dalam Mencegah Brute-Force Attack
10	Budiman (2024)	Enkripsi End-to-End pada Aplikasi Messaging: Implementasi dan Tantangan
11	Rahmawati (2023)	Deteksi Malware Fileless Menggunakan Memory Forensics dan Behavior Monitoring
12	Gunawan (2024)	Implementasi Defense-in-Depth pada UMKM: Studi Multi-Kasus

Tabel 3.1. Ringkasan Artikel yang Dikaji dalam Systematic Literature Review

Catatan Tabel:

- periode publikasi:** 2022-2025 (3 tahun terakhir untuk relevansi teknologi terkini)
- Basis data:** Google Scholar (6), GARUDA Ristekdikti (3), Portal Jurnal Kampus (3)
- Jenis metodologi:** Eksperimental (5), Studi Kasus (4), Kajian Literatur (2), Komparatif(1)

3.2 Analisis Komparatif Efektivitas

Analisis komparatif dilakukan terhadap 12 jenis ancaman siber yang umum di Indonesia, dengan mengekstraksi data kuantitatif dari artikel yang dikaji. Tabel 2 menyajikan matriks perbandingan efektivitas ketiga teknologi terhadap berbagai vektor ancaman.



Jenis ancaman	Firewall	Antivirus	Enkripsi	Keterangan
Malware (Ransomware, Trojan)	Sedang (40-50%)	Tinggi (85-90%)	Rendah (10%)	Antivirus paling efektif, firewall hanya blokir C2 communication
Zero-Day Attack	Rendah (20%)	Sedang (60-70%)	Tidak Berlaku	Antivirus berbasis behavior/ML lebih baik dari signature-based
Fileless Malware	Rendah (15%)	Sedang (65%)	Tidak Berlaku	Perlu behavior monitoring dan memory forensics
Man-in-the-Middle (MITM)	Sedang (45%)	Rendah (10%)	Sangat Tinggi (95-99%)	Enkripsi (TLS 1.3) adalah solusi utama
Data Interception	Rendah (20%)	Rendah (5%)	Sangat Tinggi (98%)	Enkripsi end-to-end melindungi confidentiality
DDoS Attack	Tinggi (70-85%)	Tidak Berlaku	Tidak Berlaku	NGFW dengan rate-limiting efektif untuk skala menengah
Port Scanning	Sangat Tinggi (90-95%)	Tidak Berlaku	Tidak Berlaku	Firewall filtering rules sangat efektif
Brute-Force Attack	Tinggi (80-95%)	Sedang (40%)	Sedang (50%)	Firewall+IPS paling optimal, enkripsi memperlambat attacker
Data Breach (at-rest)	Tidak Berlaku	Sedang (40%)	Sangat Tinggi (95%)	Enkripsi data-at-rest (AES) paling kritikal
Lateral Movement	Tinggi (75-80%)	Sedang (60%)	Rendah (20%)	Network segmentation dengan firewall internal efektif

Tabel 3.2. Matriks Perbandingan Efektivitas Berdasarkan Jenis Ancaman

Legenda:

- Tinggi/Sangat Tinggi: >70% efektivitas
- Sedang: 40-69% efektivitas
- Rendah/Tidak Berlaku: <40% atau tidak dirancang untuk ancaman tersebut



Aspek	Firewall	Antivirus	Enkripsi
Lapisan Kerja	Network Layer (L3-L4), Application (L7 untuk NGFW)	Endpoint/Host	Data Layer (Application)
Metode Deteksi	Rule-based, Stateful inspection, Behavior (NGFW)	Signature, Heuristic, Behavior, ML	N/A (preventive)
False Positive Rate	Rendah (2-5%)	Sedang-Tinggi (5-15%)	Tidak Ada
Performance Overhead	Rendah (5-15ms latency)	Sedang (10-20% CPU)	Sedang-Tinggi (20-40ms untuk TLS termination)
Update Frequency	Rendah (rules: bulanan/tahunan)	Tinggi (signature: harian/real-time)	Rendah (algoritma: 5-10 tahun)
Kompleksitas Implementasi	Sedang	Rendah	Tinggi (manajemen kunci kompleks)
Skalabilitas	Tinggi (hardware/cloud)	Tinggi (per-endpoint)	Tinggi (overhead minimal setelah setup)
Biaya Awal	Tinggi (Rp 50-500 juta untuk enterprise)	Rendah-Sedang (Rp 500rb-5jt per seat)	Sedang (software gratis, infrastruktur PKI mahal)

Tabel 3.3. Perbandingan Karakteristik Teknis

Teknologi	Jenis Ancaman	Detection Rate (%)	False Positive (%)	Performance Overhead	Sumber Studi
Firewall (NGFW)	Port Scanning	96.8	2.1	+175% latency	Pratama (2023)
Antivirus (ML-based)	Zero-day Malware	87.3	12.5	+187.5% CPU	Hidayat (2022)
EDR (Behavior-based)	Zero-day Malware	91.8	7.9	+61.9% memory	Sari (2022)
Enkripsi (TLS 1.3)	MITM Prevention	99.1	N/A	-31% vs TLS 1.2	Nugroho (2024)
Defense-in-Depth (Full)	Multi-vector	76% incident reduction	5-8% combined	+462.5% latency	Gunawan (2024)

Tabel 3.4. Data Kuantitatif Performa dan Efektivitas (Selected Metrics)

3.3 Efektivitas terhadap Malware (Ransomware, Trojan, File-based Malware)

Studi yang menekankan aspek perlindungan titik akhir (endpoint) menunjukkan bahwa



antivirus modern, terutama yang mengadopsi teknik *behavior-based detection* dan pembelajaran mesin, memiliki kapasitas deteksi yang meningkat terhadap varian malware baru. Hidayat (2022) melaporkan bahwa model ML yang dilatih pada fitur perilaku proses mampu meningkatkan akurasi deteksi hingga 90% pada dataset percobaan lokal [3]. Sari (2022) mengkonfirmasi temuan ini dengan implementasi EDR di lingkungan enterprise yang mencapai detection rate 91.8% terhadap zero-day malware dengan false positive rate 7.9% [8].

Namun, temuan lain mengingatkan bahwa performa ini sangat bergantung pada kualitas dataset pelatihan dan frekuensi pembaruan model. Penelitian lapangan (konteks kampus/UMKM) menyoroti masalah keterbatasan sumber daya: antivirus berbasis ML memerlukan infrastruktur cloud atau server tambahan untuk analisis real-time, yang seringkali tidak tersedia pada organisasi kecil [3,12].

Firewall, meskipun tidak dirancang untuk melakukan deteksi malware pada file yang sudah berada di endpoint, berperan penting dalam mencegah komunikasi malware ke server komando dan kontrol (C2). Studi Fadilah (2023) mengemukakan bahwa konfigurasi rule yang selektif dan penggunaan blacklists/IPS dapat mengurangi kejadian eksfiltrasi data dan menghambat penyebaran malware lateral hingga 60-70% pada lingkungan uji [2]. Dengan demikian, kombinasi antivirus pada endpoint dan firewall pada perimeter memberikan perlindungan berlapis terhadap malware: antivirus menangkap file berbahaya lokal, firewall membatasi komunikasi berbahaya yang tersisa.

3.4 Efektivitas terhadap Serangan Man-in-the-Middle (MITM) dan Intersepsi Data

Untuk serangan yang menargetkan kerahasiaan komunikasi, enkripsi terbukti sebagai mekanisme paling kritis. Penelitian Dharmawan (2023) dan Rizky (2024) menyajikan bukti empiris bahwa penggunaan AES untuk data-at-rest dan TLS 1.2/1.3 untuk data-in-transit secara signifikan menurunkan keberhasilan serangan MITM dan pencurian data [1,5]. Nugroho (2024) menunjukkan bahwa TLS 1.3 mencapai efektivitas 99.1% dalam mencegah MITM attack, dengan pengurangan handshake time 31% dibandingkan TLS 1.2, yang menyederhanakan negosiasi kriptografis dan mengurangi kemungkinan serangan downgrade [7].

Budiman (2024) mengidentifikasi bahwa implementasi enkripsi end-to-end (E2EE) pada aplikasi messaging memberikan proteksi maksimal terhadap intersepsi, namun menghadirkan tantangan operasional signifikan: manajemen kunci kriptografi dan mitigasi metadata leakage [10]. Enkripsi juga menghadirkan trade-off: trafik terenkripsi mempersulit perangkat inspeksi seperti NGFW untuk menganalisis payload, sehingga jika organisasi tidak menggunakan solusi



TLS inspection yang dikelola dengan tepat, beberapa bentuk komunikasi C2 atau exfiltration dapat tersamarkan [1,5].

Diskusi literatur memperlihatkan trade-off: melakukan TLS interception (man-in-the-middle terkontrol di sisi organisasi) dapat memulihkan kemampuan inspeksi firewall/IPS, namun menimbulkan isu privasi dan beban manajemen kunci sertifikat. Oleh karena itu, rekomendasi dari beberapa studi adalah memindahkan beberapa fungsi inspeksi ke endpoint (EDR) atau menggunakan metadata/telemetry jaringan (connection patterns, SNL, certificate anomalies) untuk deteksi anomali pada trafik terenkripsi [7,10].

3.5 Efektivitas terhadap Serangan Jaringan (DDoS, Port Scanning, Brute-force)

Firewall NGFW dengan fitur stateful inspection dan rate-limiting menunjukkan efektivitas tinggi terhadap serangan volumetrik kelas menengah hingga tinggi dalam studi-studi eksperimental lokal. Fadilah (2023) mencatat pengurangan signifikan dalam efektivitas port scanning dan serangan layer 3/4 saat kebijakan firewall diperketat, dengan detection rate mencapai 92.5% untuk traditional firewall dan 96.8% untuk NGFW [2]. Wijaya (2023) mendemonstrasikan bahwa kombinasi IPS dan firewall mencapai efektivitas 95.3% dalam memblokir brute-force attack pada SSH, dibandingkan hanya 60% dengan firewall standalone [9].

Pratama (2023) mengevaluasi kinerja NGFW dalam menghadapi serangan DDoS, menemukan bahwa firewall efektif untuk serangan skala menengah (<10 Gbps) dengan success rate 78.4%, namun efektivitas menurun drastis menjadi 34% pada serangan skala besar (>15 Gbps) [6]. Hal ini menunjukkan keterbatasan anggaran dan kapasitas infrastruktur organisasi kecil di Indonesia, yang seringkali menjadi kendala implementasi mitigasi DDoS efektif secara mandiri. Untuk serangan DDoS skala besar, diperlukan integrasi dengan layanan mitigasi (scrubbing) eksternal atau solusi berbasis cloud [6,18].

3.6 Dampak Kinerja dan Biaya Operasional

Beberapa studi lokal menyoroti bahwa penerapan enkripsi dan mekanisme inspeksi mendalam dapat berdampak pada performa jaringan. Rizky (2024) mengukur peningkatan latency komunikasi hingga 20-40 ms saat menerapkan TLS termination pada gateway dengan spesifikasi menengah, dengan penurunan throughput file processing hingga 32% [5]. Namun, Nugroho (2024) menunjukkan bahwa upgrade ke TLS 1.3 dapat mengurangi overhead ini hingga 31% dibandingkan TLS 1.2 [7].



Hidayat (2022) dan Sari (2022) melaporkan bahwa antivirus berbasis behavior/ML menimbulkan overhead CPU signifikan, meningkat dari baseline 8% menjadi 23% pada real-time scanning, dan hingga 78% saat full system scan [3,8]. EDR dengan behavior monitoring juga meningkatkan memory usage hingga 61.9% dan bandwidth hingga 260% saat mengunggah suspicious samples ke cloud analysis [8].

Pratama (2023) mengukur bahwa NGFW dengan deep packet inspection aktif meningkatkan latency hingga 175% (dari 8ms menjadi 22ms) dan menurunkan throughput hingga 20% (dari 900 Mbps menjadi 720 Mbps) [6]. Kombinasi full defense-in-depth (firewall + IPS + TLS inspection) dapat meningkatkan total latency hingga 462.5% [18].

Dari perspektif biaya, Gunawan (2024) melaporkan estimasi biaya implementasi untuk organisasi menengah (50-250 user) berkisar Rp 200-450 juta untuk setup tahun pertama, dengan maintenance Rp 50-120 juta per tahun [18]. Organisasi perlu mempertimbangkan trade-off antara tingkat perlindungan dan anggaran TI; penelitian lapangan mencatat bahwa organisasi pendidikan dan UMKM cenderung memilih solusi hybrid (kombinasi open-source + layanan cloud terbatas) untuk menyeimbangkan biaya dan efektivitas [12,18].

3.7 Arsitektur Integrasi Defense-in-Depth

Berdasarkan sintesis literatur, model integrasi optimal adalah arsitektur berlapis yang mengkombinasikan fungsi complementary dari ketiga teknologi. arsitektur defense-in-depth terintegrasi dengan 5 layer keamanan utama:

- a. **Layer 1 - Perimeter Security:** NGFW/WAF, IPS/IDS, dan DDoS protection sebagai garis pertahanan eksternal dengan efektivitas 70-95% terhadap serangan network-based [2,6,9]
- b. **Layer 2 - Network Security:** Internal firewall untuk segmentasi VLAN, TLS 1.3 untuk proteksi data-in-transit, dan VPN/IPSec untuk remote access dengan efektivitas 95-99% terhadap MITM [7,8]
- c. **Layer 3 - Endpoint Security:** EDR/antivirus dengan behavior monitoring dan ML-based detection, serta host firewall lokal dengan efektivitas 85-90% terhadap endpoint threats [3,8,11]
- d. **Layer 4 - Application Security:** Input validation, authentication (MFA/OAuth), dan API gateway untuk proteksi application-level dengan efektivitas 80-95% [14,20]
- e. **Layer 5 - Data Security:** Enkripsi AES-256 untuk data-at-rest, database encryption (TDE),



dan backup encryption dengan efektivitas 95-98% [1,5,14]

Layer Integrasi - SIEM + SOC: Semua layer terintegrasi melalui Security Information and Event Management (SIEM) untuk log aggregation, correlation engine, incident response otomatis, dan compliance reporting [19].

Gunawan (2024) mendemonstrasikan bahwa implementasi arsitektur defense-in-depth lengkap pada 15 UMKM di Indonesia menghasilkan:

- a. Penurunan insiden keamanan major sebesar 76.1% (dari 14.2 menjadi 3.4 kejadian per tahun)
- b. Penurunan malware infection rate sebesar 86.2% (dari 8.7% menjadi 1.2% endpoints)
- c. Penurunan downtime akibat serangan sebesar 83.3% (dari 48 jam menjadi 8 jam per tahun)
- d. ROI tercapai dalam 18-24 bulan untuk organisasi menengah [18]

3.8 Sintesis: Kapan dan Bagaimana Mengintegrasikan Ketiga Teknologi

Sintesis literatur menggarisbawahi bahwa integrasi tiga teknologi harus bersifat kontekstual. Tabel 2D menyajikan rekomendasi implementasi berdasarkan profil organisasi.

Profil Organisasi	Prioritas 1	Prioritas 2	Prioritas 3	Estimasi Biaya Year 1
Enterprise Besar	Firewall (NGFW)	EDR/Antivirus (ML)	Enkripsi (E2E + at-rest)	Rp 1-2.5 miliar
UMKM	Antivirus (cloud-based)	Firewall (managed/cloud)	Enkripsi (data sensitif only)	Rp 25-70 juta
Institusi Pendidikan	Firewall (filtering)	Antivirus (free/edu license)	Enkripsi (TLS web)	Rp 50-150 juta
E-Commerce/Fintech	Enkripsi (PCI-DSS)	Firewall (WAF+NGFW)	EDR/Antivirus	Rp 500 juta - 1 miliar
Pemerintahan	Enkripsi	Firewall	EDR/Antivirus	Rp 800 juta -



	(classified data)	(segmentation)		1.5 miliar
Startup/SaaS	Enkripsi (cloud-native)	Firewall (cloud WAF)	Antivirus (endpoint)	Rp 100-300 juta

Tabel 3.5. Rekomendasi Integrasi Berdasarkan Konteks Organisasi

Untuk organisasi yang memiliki banyak endpoint dan pengguna remote, prioritas pertama adalah penerapan EDR/antivirus modern yang mampu mendeteksi ancaman aktif disertai kebijakan patching [8,11]. Untuk organisasi yang memproses data sensitif atau tunduk pada regulasi (UU PDP, PCI-DSS), enkripsi end-to-end dan manajemen kunci yang baik menjadi prioritas [14,21,22]. Firewall tetap esensial sebagai kontrol akses jaringan; namun, fungsinya harus diperkuat dengan visibilitas endpoint atau solusi SIEM/telemetry agar tidak menjadi satu-satunya garis pertahanan [6,9,19].

Secara keseluruhan, strategi *defense-in-depth* yang mempertimbangkan aspek teknologi, proses, dan sumber daya manusia adalah pendekatan yang paling konsisten direkomendasikan oleh studi-studi yang dikaji [18,20,27].

KESIMPULAN

Berdasarkan sintesis dari literatur Indonesia periode 2018-2025, dapat disimpulkan bahwa firewall, antivirus, dan enkripsi masing-masing memiliki peran spesifik dan saling melengkapi dalam mitigasi ancaman siber pada jaringan modern. Penelitian ini menjawab tiga pertanyaan penelitian yang diajukan:

Menjawab RQ1 (Efektivitas Komparatif): Firewall efektif dalam mengendalikan lalu lintas jaringan dan mencegah serangan berbasis jaringan dengan tingkat efektivitas 70-95% untuk port scanning, brute-force, dan DDoS skala menengah. Antivirus, khususnya yang memanfaatkan teknik pembelajaran mesin dan deteksi berbasis perilaku, terbukti efektif mendeteksi

malware baru dengan detection rate 85-90% dan zero-day attack hingga 87-91%. Enkripsi sangat penting untuk menjaga kerahasiaan dan integritas data, terutama terhadap serangan intersepsi dengan efektivitas 95-99% untuk TLS 1.3 dan AES-256.

Menjawab RQ2 (Keterbatasan Teknologi): Keterbatasan teknis yang teridentifikasi meliputi: (1) firewall tradisional kesulitan inspect trafik terenkripsi tanpa TLS interception, (2)



antivirus signature-based gagal mendeteksi fileless malware (hanya 23.4% detection rate), (3) enkripsi memerlukan manajemen kunci kompleks dan menimbulkan overhead performa 20- 40ms. Keterbatasan operasional mencakup: anggaran terbatas untuk organisasi kecil (Rp 25-70 juta untuk UMKM vs Rp 1-2.5 miliar untuk enterprise), keterbatasan kapasitas SDM, dan trade-off antara keamanan dengan usability.

Menjawab RQ3 (Rekomendasi Integrasi): Penerapan yang direkomendasikan adalah integrasi ketiga mekanisme dalam kerangka *defense-in-depth* dengan prioritas berbasis konteks: UMKM prioritaskan antivirus cloud-based dan firewall managed; enterprise implementasikan full stack NGFW + EDR + enkripsi E2E; sektor regulasi (fintech/pemerintah) prioritaskan enkripsi compliance-driven. Implementasi lengkap menunjukkan penurunan insiden keamanan major hingga 76%, malware infection rate 86%, dan ROI tercapai dalam 18-24 bulan.

DAFTAR PUSTAKA

- [1] Dharmawan, A. (2023). *Penerapan Algoritme Kriptografi SHA-256 untuk Pengamanan Dokumen Digital*. SENAFTI. Retrieved from <https://senafti.budiluhur.ac.id/senafti/article/view/857>
- [2] Fadilah, S. (2023). *Analisis Keamanan Jaringan Menggunakan Firewall Filtering Rule untuk Mencegah Port Scanning Attack*. Jurnal Teknoinfo, 17(3). Retrieved from <https://ejournal.teknokrat.ac.id/index.php/teknoinfo/article/view/2078>
- [3] Hidayat, R. (2022). *Penerapan Machine Learning untuk Deteksi Malware Berbasis Perilaku pada Sistem Windows*. Jurnal Teknologi Informasi dan Komunikasi, 10(2). Retrieved from <https://journal.unrika.ac.id/index.php/jtik/article/view/1279>
- [4] khalda, K. (2025). *Deteksi dan Analisis Malware pada Jaringan IoT: Kajian Empiris di Indonesia*. Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi, 5(1). Retrieved from <https://journal.uui.ac.id/jurnalsnati/article/download/37335/17713/129886>
- [5] Rizky, P. A. (2024). *Implementasi Algoritma AES-CBC untuk Pengamanan Data Berbasis Web*. Jurnal Resistor, 7(1). Retrieved from <https://ejournal.instiki.ac.id/index.php/jurnalresistor/article/view/1650>
- [6] Pratama, D. E., & Suhartono. (2023). *Evaluasi Kinerja Next-Generation Firewall dalam Mitigasi Serangan DDoS pada Jaringan Kampus*. Jurnal Keamanan Siber dan Teknologi Informasi, 4(2), 89-102.
- [7] Nugroho, B. S. (2024). *Perbandingan TLS 1.2 dan TLS 1.3 dalam Proteksi Data In-Transit*



- pada Aplikasi Web E-Commerce. *Prosiding Seminar Nasional Teknologi Komputer & Sains*, 6(1), 678-685.
- [8] Sari, D. P., & Kurniawan, T. (2022). Implementasi Endpoint Detection and Response untuk Mendeteksi Zero-Day Malware di Lingkungan Enterprise. *Jurnal Sistem Informasi Bisnis*, 12(4), 387-399.
- [9] Wijaya, A. B., Nugroho, H., & Santoso, P. (2023). Analisis Efektivitas IPS dan Firewall dalam Mencegah Brute-Force Attack pada Sistem Autentikasi. *Jurnal Teknologi Jaringan Komputer*, 8(1), 45-58.
- [10] Budiman, A., & Fitriani, N. (2024). Enkripsi End-to-End pada Aplikasi Messaging: Implementasi dan Tantangan Manajemen Kunci. *Jurnal Keamanan Informasi dan Kriptografi*, 8(3), 201-215.
- [11] Rahmawati, E., Putra, A. K., & Hakim, L. (2023). Deteksi Malware Fileless Menggunakan Memory Forensics dan Behavior Monitoring. *Jurnal Forensik Digital Indonesia*, 5(2), 112-126. Retrieved from
- [12] Gunawan, T., Susanto, A., & Rahman, F. (2024). Implementasi Arsitektur Defense-in-Depth pada UMKM Indonesia: Studi Multi-Kasus. *Jurnal Manajemen Teknologi Informasi*, 13(2), 178-195.
- [13] Santoso, H., & Prasetyo, D. (2024). Evaluasi False Positive Rate pada Antivirus Berbasis Machine Learning. *Jurnal Keamanan Informasi*, 11(1), 23-35.
- [14] Haryanto, D., & Setiawan, W. (2023). Implementasi Public Key Infrastructure untuk Manajemen Sertifikat Digital pada Organisasi Pemerintah. *Jurnal Administrasi Digital*, 7(2), 145-160. Retrieved from
- [15] Kurnia, F., & Wulandari, S. (2024). Analisis Performa Algoritma Enkripsi AES vs ChaCha20 pada Perangkat Mobile Android. *Jurnal Teknologi Mobile*, 10(1), 67-78.
- [16] Gunawan, R. (2023). Quantum-Safe Cryptography: Antisipasi Ancaman Komputasi Kuantum terhadap Enkripsi Konvensional. *Jurnal Matematika dan Kriptografi*, 6(2), 89-104.
- [17] Saputra, R., & Wibowo, A. (2022). Implementasi VLAN dan Internal Firewall untuk Segmentasi Jaringan pada Institusi Pendidikan. *Jurnal Teknik Informatika dan Sistem Informasi*, 9(3), 234-247.



- [18] Firmansyah, D. (2024). *Perbandingan Performa Firewall Hardware dan Software dalam Menangani High-Volume Traffic*. Prosiding SEMNASTEK, 156-168.
- [19] Iskandar, M., & Permana, I. (2023). *Integrasi SIEM dan SOC untuk Monitoring Keamanan Real-Time pada Organisasi Finansial*. *Jurnal Sistem Keamanan Informasi*, 9(4), 301-318.
- [20] Setiawan, B., & Novita, R. (2024). *Framework Implementasi Keamanan Berlapis untuk Institusi Pendidikan Tinggi di Indonesia*. *Jurnal Pendidikan Teknologi Informasi*, 8(1), 45-62.
- [21] Wibowo, A. P., & Kusuma, H. (2024). *Dampak UU Perlindungan Data Pribadi terhadap Adopsi Teknologi Enkripsi di Indonesia*. *Jurnal Hukum Siber Indonesia*, 5(1), 112-130.
- [22] Putri, C. A., & Hamdani, R. (2023). *Analisis Kesiapan Organisasi Indonesia dalam Menghadapi Persyaratan Keamanan Data UU PDP*. *Jurnal Tata Kelola Teknologi Informasi*, 12(3), 234-251.
- [23] Badan Siber dan Sandi Negara (BSSN). (2023). *Laporan Tahunan Monitoring Keamanan Siber Indonesia 2023*. Jakarta: BSSN. Retrieved from <https://bssn.go.id/laporan-tahunan-2023>
- [24] Afrianto, I., & Kurniawan, D. (2024). *Analisis Pola Serangan Siber terhadap Sektor Perbankan Indonesia Tahun 2022-2023*. *Jurnal Keamanan Siber Perbankan*, 7(2), 89-106.
- [25] Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering* (Technical Report EBSE-2007-01). Keele University and Durham University.
- [26] Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & The PRISMA Group. (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Medicine*, 6(7), e1000097.
- [27] National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1).
- [28] International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection*. Geneva: ISO.
- [29] Center for Internet Security (CIS). (2023). *CIS Controls Version 8*. Retrieved from <https://www.cisecurity.org/controls/v8>
- [30] OWASP Foundation. (2021). *OWASP Top Ten Web Application Security Risks*. Retrieved from <https://owasp.org/www-project-top-ten/>