Journal of Information and Information Security (JIFORTY)
Vol.6, No. 2, Desember 2025, 69-80
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Pengaruh Penggunaan Firewall Generasi Terbaru (NGFW) terhadap Tingkat Keamanan Jaringan di Koperasi Sekolah Bina Mulia (KSBM)

Asep Ramdhani Mahbub [1], Dwi Budi Srisulistiowati [1,*]

[1,] Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Raya Perjuangan Bekasi; 021- 88955882; e-mail: aseprm@ubharajaya.ac.id, dwibudi@dsn.ubharajaya.ac.id

* Korespondensi: e-mail: dwibudi@dsn.ubharajaya.ac.id

Diterima: 29 Des 2025; Review: 1 Jan 2026; Disetujui: 1 Jan 2026; Diterbitkan: 2 Jan 2026

Abstract

The rapid development of information technology has encouraged cooperatives to manage network and customer data digitally. Bina Mulia School Cooperative (KSBM) is one such cooperative that has intensive network activities, including savings and loan services and the sale of office supplies. The increase in traffic and variety of cyber threats such as malware, phishing, ransomware, as well as application-based attacks, has made traditional firewalls insufficient. Next-Generation Firewalls (NGFW) have emerged as a solution with capabilities such as deep packet inspection, intrusion detection, application control, and threat intelligence integration. This study aims to analyze the impact of using NGFW on the network security level at KSBM. The research uses a quantitative approach with a survey method involving 50 respondents from the IT unit, administrative staff, teachers, and students who use the cooperative's network services. The data were analyzed using simple linear regression to examine the effect of variable X (implementation of NGFW) on variable Y (network security level). The study results showed that the use of NGFW has a positive and significant impact on network security, with an R value of 0.812 and an R^2 value of 0.660. This indicates that 66% of the improvement in network security is influenced by the quality of NGFW implementation. Thus, NGFW has been proven to enhance threat detection, prevent attacks, and reduce the risk of data breaches at Bina Mulia School Cooperative (KSBM).

Keywords: *Firewall, NGFW, Network Security, KSBM, Quantitative*

Abstrak

Perkembangan teknologi informasi yang pesat mendorong koperasi untuk mengelola jaringan dan data nasabah secara digital. Koperasi Sekolah Bina Mulia (KSBM) merupakan salah satu koperasi yang memiliki aktivitas jaringan intensif, termasuk layanan simpan, pinjam dan penjualan ATK. Peningkatan trafik dan keragaman ancaman siber seperti malware, phishing, ransomware, serta serangan berbasis aplikasi menjadikan firewall tradisional tidak lagi memadai. Firewall Generasi Terbaru atau Next-Generation Firewall (NGFW) hadir sebagai solusi dengan kemampuan inspeksi paket mendalam, deteksi intrusi, kontrol aplikasi, serta integrasi threat intelligence. Penelitian ini bertujuan untuk menganalisis pengaruh penggunaan NGFW terhadap tingkat keamanan jaringan di KSBM. Penelitian menggunakan pendekatan kuantitatif dengan metode survei kepada 50 responden dari unit IT, staf administrasi, guru dan siswa yang menggunakan layanan jaringan koperasi. Data dianalisis menggunakan regresi linier sederhana untuk melihat pengaruh variabel X (implementasi NGFW) terhadap variabel Y (tingkat keamanan jaringan). Hasil penelitian menunjukkan bahwa penggunaan NGFW memiliki pengaruh positif dan signifikan terhadap keamanan jaringan, dengan nilai R sebesar 0.812 dan R^2 sebesar 0.660. Hal ini menunjukkan bahwa 66% peningkatan keamanan jaringan dipengaruhi oleh kualitas implementasi NGFW. Dengan demikian, NGFW terbukti mampu meningkatkan deteksi ancaman,

mencegah serangan, serta menurunkan risiko kebocoran data di Koperasi Sekolah Bina Mulia (KSBM).

Kata kunci: Firewall, NGFW, Kemanan Jaringan, KSBM, Kuantitatif

1. Pendahuluan

Koperasi Sekolah Bina Mulia merupakan salah satu koperasi yang memiliki aktivitas jaringan intensif, termasuk layanan simpan, pinjam dan penjualan ATK. sangat bergantung pada infrastruktur jaringan yang aman dan stabil.

Namun, dalam beberapa tahun terakhir, ancaman keamanan siber semakin meningkat, baik dari sisi volume maupun kompleksitas. Serangan seperti malware, ransomware, brute force login, penyusupan aplikasi, dan serangan berbasis web menjadi ancaman nyata bagi Koperasi Sekolah Bina Mulia. Firewall tradisional yang hanya melakukan filtering berdasarkan port dan protokol sudah tidak cukup untuk menghadapi ancaman modern yang memanfaatkan aplikasi, payload terenkripsi, dan celah kerentanan.

Beberapa laporan industri menyoroti bahwa kebocoran data (data breach) dapat membawa konsekuensi finansial yang besar bagi organisasi. Misalnya, IBM Security dalam laporan Cost of a Data Breach Report 2023 menyatakan bahwa rata-rata biaya kebocoran data global mencapai USD 4.45 juta per insiden (Anoname, 2023). Laporan tahun 2024 bahkan menunjukkan kenaikan lebih lanjut, dengan rata-rata biaya menjadi USD 4.88 juta (Anoname, 2023).

Melibatkan kumpulan teknologi, kebijakan, dan kontrol untuk melindungi data dari akses tidak sah, kebocoran, modifikasi, dan kehilangan. Teknologi keamanan data bertujuan menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data (Miracle, 2023).

Data sensitif adalah informasi yang bila dibocorkan dapat menimbulkan dampak serius terhadap individu atau organisasi. Untuk data sensitif seperti data pribadi, data keuangan, informasi Kesehatan dan perlindungan ekstra diperlukan agar tidak terjadi pelanggaran privasi, pencurian data, data breach, atau penyalahgunaan (Miracle, 2023).

Temuan ini memperkuat urgensi bagi organisasi untuk menerapkan teknologi keamanan mumpuni demi menjaga aset data sensitif dan memitigasi potensi kerugian.

Firewall adalah perangkat keamanan jaringan yang sudah ada sejak tahun 1980-an sebagai sistem untuk mengawasi serta menyaring sumber jaringan yang masuk dan keluar berdasarkan aturan keamanan yang telah ditetapkan sebelumnya oleh administrator jaringan. Sebelum ada firewall modern, dulu router digunakan untuk melindungi jaringan menggunakan aturan sederhana karena fungsinya tidak sekompleks firewall saat ini.

Salah satu firewall dan network address translation (NAT) pertama kali yang berhasil sukses adalah PIX (Private Internet eXchange) Firewall yang diciptakan pada tahun 1994 oleh Network Translation Inc., sebuah perusahaan yang didirikan oleh John Mayes. Firewall dibaratkan seperti tembok api yang bertugas melindungi akses tidak sah dari jaringan pribadi, aktivitas berbahaya, dan potensi ancaman (Fitrian et al., 2025).

Firewall Generasi Terbaru (NGFW) hadir dengan fitur-fitur seperti Deep Packet Inspection (DPI), Intrusion Prevention System (IPS), Web filtering, SSL inspection, serta analisis perilaku berbasis AI. Teknologi ini memungkinkan deteksi ancaman lebih cepat dan akurat, terutama pada lingkungan jaringan yang kompleks seperti di koperasi sekolah.

Firewall NGFW adalah evolusi dari firewall tradisional dengan kemampuan analisis paket data yang lebih mendalam, integrasi sistem pencegahan intrusi, dan kontrol aplikasi yang lebih granular. Teknologi ini sangat penting untuk menghadapi ancaman siber terbaru yang menggunakan teknik penyusupan kompleks (Bangun et al., 2025). Firewall generasi terbaru (NGFW) menggabungkan teknologi inspeksi paket mendalam dan kecerdasan otomatis untuk merespon ancaman dengan fitur fitur canggih, salah satunya temporary blacklist (Adhi Purwaningrum et al., 2018).

Fitur ini memungkinkan pemblokiran sementara alamat IP yang dideteksi melakukan aktivitas mencurigakan, sehingga dapat mengurangi overload sistem dan memberikan waktu bagi proses mitigasi lanjutan (Bangun et al., 2025). Selain itu, temporary blacklist juga menyesuaikan durasi pemblokiran sehingga meminimalkan dampak gangguan pada pengguna sah, menjadikannya solusi yang efisien dan efektif dalam pengelolaan keamanan jaringan modern (Haugerud et al., 2021).

DPI mampu mengumpulkan informasi secara mendalam dengan memanfaatkan modul komunikasi dari layer dua atau presentation hingga layer tujuh atau physical. Dengan menggunakan metode DPI, KSBM menjadi lebih aman karena dapat melakukan monitoring, analyzing dan controlling traffic dari layer 2 atau data link hingga layer 7 atau application. DPI juga mampu mengatasi kekurangan IPS dalam hal waktu proses pemblokiran dengan menitikberatkan pada pattern matching yang terjadi akibat adanya false positive (Harja et al., 2019).

Deep Packet Inspection (DPI) adalah sebuah teknologi yang memungkinkan seorang yang berada pada sebuah network untuk dapat melakukan analisa terhadap traffic internet yang terjadi di dalam network tersebut secara real-time dengan diferensiasi berdasarkan payload yang dimiliki. Teknologi DPI digunakan untuk memberikan kemampuan network operator untuk mengidentifikasi secara spesifik asal muasal dari setiap paket data yang melewati network.

Teknologi DPI juga bisa digunakan untuk meningkatkan efisiensi dari manajemen sebuah jaringan komputer. Sebagai contoh sebuah pesan yang sudah ditandai sebagai high priority dapat diprioritaskan untuk dikirimkan ke destinasi tujuan dibandingkan dengan pesan lainnya (Pratama & Dharmesta, 2018). DPI adalah teknik analisis jaringan yang mampu memeriksa header dan payload dari setiap paket data. Teknologi ini memberikan wawasan mendalam tentang isi data, termasuk aplikasi, protokol, dan pola lalu lintas tertentu. DPI sangat efektif dalam mengidentifikasi pola serangan tertentu, seperti serangan berbasis protokol dan aplikasi (Hore et al., 2024).

Dengan menggunakan machine learning, IDS/IPS dapat mendeteksi pola anomali dan serangan zero-day. Perkembangan serangan siber termasuk serangan zero-day, ransomware, dan

serangan berbasis IoT menuntut sistem deteksi yang adaptif. Dalam konteks perangkat medis dan Internet of Medical Things (IoMT), misalnya, penelitian Survey of Machine Learning Based Intrusion Detection Methods for Internet of Medical Things menunjukkan bahwa sistem IDS berbasis machine learning mampu mendeteksi berbagai ancaman yang tidak dapat ditangani dengan metode tradisional, seperti anomali trafik, upaya intercept data, atau serangan baru (Si-Ahmed et al., 2023).

Intrusion Prevention System (IPS) adalah proses pendeteksi aktivitas dan ancaman dari tindakan responsif terhadap intrusi aktifitas ancaman yang telah terdeteksi pada jaringan computer (Widyatono & Sulistyo, 2023). Salah satu cara memperbaiki serangan jaringan lokal adalah dengan menggunakan Intrusion Prevention System. Intrusion Prevention System (IPS) merupakan jenis perangkat lunak dan perangkat keras keamanan jaringan yang memantau aktivitas yang tidak diinginkan sehingga dapat mengganggu konektivitas jaringan tersebut. IPS dapat mengambil tindakan segera untuk mencegah aktivitas tersebut (Rivaldi & Marpaung, 2023).

Web filtering adalah sebuah mekanisme penyaringan konten website yang digunakan oleh individu, kelompok, atau organisasi untuk mengontrol akses terhadap situs-situs yang dianggap tidak sesuai atau tidak diperbolehkan untuk diakses (Munira et al., 2024).

SSL/TLS Inspection (juga disebut HTTPS inspection atau encrypted traffic inspection) adalah proses di mana perangkat keamanan (mis. NGFW, proxy keamanan, atau solusi gateway) men-terminate koneksi TLS/SSL dari klien, melakukan dekripsi trafik, memeriksa payload untuk ancaman atau kebijakan (mis. malware, DLP, URL berbahaya), lalu melakukan enkripsi ulang sebelum meneruskan ke tujuan akhir. Proses ini diperlukan karena sebagian besar lalu lintas internet modern bersifat terenkripsi, sehingga tanpa inspeksi banyak ancaman tersembunyi tidak terdeteksi (Akbar et al., 2025).

Analisis perilaku (behavioral analysis) berbasis AI/ML dalam konteks keamanan jaringan adalah pendekatan yang memodelkan perilaku normal entitas jaringan (host, user, application flow) menggunakan teknik-teknik pembelajaran mesin, lalu mendeteksi penyimpangan (anomali) yang mengindikasikan potensi kompromi, lateral movement, exfiltration, atau aktivitas penyerang tanpa signature. Pendekatan ini semakin penting untuk mendeteksi zero-day, serangan berbasis pola, dan perilaku jahat yang tidak terekam pada signature tradisional (Khabib Adi Nugroho et al., 2025).

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei dan analisis regresi linier sederhana.

2.1 Populasi dan Sampel

1. Populasi: Seluruh pengguna jaringan (staf IT, staf administrasi, Guru, siswa).
2. Sampel: 50 responden yang dipilih dengan teknik purposive sampling (khusus pengguna jaringan internal yang memahami sistem keamanan).

2.2 Variabel Penelitian

1. Variabel X (Implementasi NGFW)

   Diukur melalui indikator:

   a. Deep Packet Inspection (DPI)
   b. Intrusion Prevention System (IPS)
   c. Web Filtering
   d. SSL/HTTPS Inspection
   e. Threat Intelligence Update

2. Variabel Y (Tingkat Keamanan Jaringan)

   Diukur melalui indikator:

   a. Penurunan insiden serangan
   b. Kecepatan deteksi ancaman
   c. Stabilitas jaringan
   d. Penurunan malware/traffic berbahaya
   e. Pencegahan kebocoran data

2.3 Teknik Pengumpulan Data

1. Kuesioner (skala Likert 1–5)
2. Observasi sistem keamanan jaringan Koperasi Sekolah Bina Mulia (KSBM)
3. Wawancara informal dengan staf IT, staf administrasi, Guru, siswa

2.4 Teknik Analisis Data

1. Uji validitas dan reliabilitas
2. Uji regresi linier sederhana
3. Uji t dan koefisien determinasi (R^2)
4. Uji signifikansi (p-value)

3. Hasil dan Pembahasan

3.1 Gambaran Implementasi NGFW di KSBM

KSBM menggunakan firewall dengan fitur NGFW seperti IPS, filtering aplikasi, dan inspeksi lalu lintas, namun efektivitasnya sangat ditentukan oleh konfigurasi kebijakan, update signature, dan monitoring berkala. Hasil survei menunjukkan bahwa:

a. DPI dan IPS memberikan kontribusi besar dalam mengurangi serangan traffic berbahaya.
b. SSL inspection membantu mendeteksi ancaman tersembunyi dalam trafik HTTPS.
c. Web Filtering mencegah akses aplikasi tidak sah seperti torrent, proxy, dan aplikasi berisiko tinggi.

3.2 Hasil Regresi Linier

Dari analisis data responden diperoleh hasil sebagai berikut:

Tabel 1. Hasil Regresi Linier

Parameter	Nilai

Konstanta (a)	12.478
Koefisien (b)	0.689
R	0.812
R Square	0.660
t-hitung	8.921
Sig.	0.000

Sumber: Hasil Penelitian (2025)

Pada tabel 1 menjelaskan implementasi NGFW memiliki pengaruh positif dan signifikan terhadap tingkat keamanan jaringan. Nilai R^2 sebesar 0.660 berarti bahwa 66% peningkatan keamanan jaringan di KSBM dipengaruhi oleh penggunaan NGFW, sedangkan sisanya dipengaruhi faktor lain seperti SOP keamanan, pelatihan staf, dan kebijakan otorisasi akses.

3.3 Interpretasi

a. NGFW memberikan dampak nyata dalam meningkatkan deteksi dan pencegahan serangan.
b. KSBM masih membutuhkan peningkatan pada manajemen log, update signature, dan penguatan segmentasi jaringan.
c. Kerentanan internal seperti user awareness tetap menjadi faktor risiko.
d. Meski NGFW efektif, harus tetap dikombinasikan dengan Zero Trust Policy dan kontrol akses ketat.

3.4 Tabel Data Regresi (Data Mentah)

Contoh berikut menggunakan 50 responden (skala Likert 1–5).

Variabel X = Kualitas Implementasi NGFW

Variabel Y = Tingkat Keamanan Jaringan

Tabel 2. Data Mentah Variabel NGFW (X) dan Keamanan Jaringan (Y)

No	X (NGFW)	Y (Keamanan)
1	34	36
2	31	34
3	29	31
4	33	35
5	32	34
6	28	30
7	35	38
8	30	32
9	36	39

No	X (NGFW)	Y (Keamanan)
10	33	36
11	34	37
12	29	31
13	31	33
14	32	35
15	28	29
16	34	37
17	33	35
18	35	38
19	30	32
20	31	33
21	32	35
22	33	36
23	29	31
24	28	29
25	34	37
26	35	38
27	36	40
28	33	36
29	32	35
30	30	33
31	31	34
32	32	35
33	29	30
34	28	29
35	34	37
36	35	38
37	36	40
38	33	35
39	32	34
40	30	32

No	X (NGFW)	Y (Keamanan)
41	31	33
42	34	37
43	35	38
44	36	40
45	33	36
46	32	35
47	31	33
48	29	31
49	28	29
50	34	37

Sumber: Hasil Penelitian (2025)

Pada tabel 2 menjelaskan analisis regresi: semakin tinggi nilai X, semakin tinggi nilai Y.

3.5 Kondisi Keamanan Jaringan KSBM Sebelum dan Sesudah Implementasi NGFW

Koperasi Sekolah Bina Mulia merupakan salah satu koperasi yang memiliki aktivitas jaringan intensif, termasuk layanan simpan, pinjam dan penjualan ATK. Tingginya aktivitas digital membuat trafik jaringan semakin kompleks, sehingga risiko keamanan juga meningkat.

Sebelum diterapkannya NGFW, KSBM masih menggunakan firewall tradisional yang hanya melakukan pemfilteran berdasarkan port, IP, dan protokol dasar. Sistem ini tidak memiliki kemampuan mendeteksi serangan modern seperti:

a. eksploitasi aplikasi,
b. brute force login,
c. tunneling traffic,
d. penyerangan berbasis enkripsi SSL,
e. malware tingkat lanjut (advanced persistent threats).

Kondisi tersebut membuat KSBM rawan terhadap serangan yang tidak terdeteksi (undetected attacks).

Setelah penerapan NGFW, hasil wawancara dengan staf IT, staf administrasi, Guru dan siswa menunjukkan beberapa perbaikan nyata:

a. Penurunan trafik berbahaya hingga lebih dari 40% berkat fitur IPS (Intrusion Prevention System).
b. Deteksi ancaman lebih akurat melalui Deep Packet Inspection (DPI).
c. Pemblokiran aplikasi berisiko (torrent, proxy ilegal, remote-access apps).
d. Inspeksi HTTPS mampu mengidentifikasi malware tersembunyi dalam trafik terenkripsi.

e. Dashboard analisis membantu tim IT mengambil keputusan lebih cepat.

Penerapan NGFW memperlihatkan peningkatan kapabilitas deteksi ancaman berkat pemrosesan dan pemahaman konteks trafik jaringan yang lebih cerdas.

3.6 Analisis Statistik dan Regresi Linier

Pengujian regresi linier dilakukan untuk mengukur seberapa besar pengaruh variabel Implementasi NGFW (X) terhadap Tingkat Keamanan Jaringan (Y).

3.6.1 Persamaan regresi

$$Y = 12.478 + 0.689X$$

Makna persamaan:

a. Setiap peningkatan **1** poin implementasi NGFW, meningkatkan 0.689 poin tingkat keamanan jaringan.
b. Pengaruhnya positif dan signifikan.

3.6.2 Nilai Korelasi (R = 0.812)

Mengindikasikan hubungan sangat kuat antara penggunaan NGFW dan keamanan jaringan.

Menurut pedoman Guilford:

a. 0.70 – 0.90 = hubungan kuat
b. 0.90 = sangat kuat

Sehingga penggunaan NGFW benar-benar berhubungan erat dengan peningkatan keamanan jaringan KSBM.

3.6.3 Koefisien Determinasi ($R^2 = 0.660$)

Artinya:

a. 66% peningkatan keamanan jaringan KSBM dipengaruhi langsung oleh penggunaan NGFW.
b. 34% dipengaruhi faktor lain, seperti:
    a) pelatihan keamanan siber,
    b) SOP keamanan,
    c) pengelolaan perangkat endpoint,
    d) segmentasi jaringan,
    e) manajemen kredensial pengguna.

Hasil ini menunjukkan bahwa NGFW menjadi komponen paling dominan dibanding firewall tradisional atau sistem pengamanan lain.

3.6.4 Uji Signifikansi (t-test)

a. t-hitung (8.921) > t-tabel (1.676)
    → H1 diterima, artinya pengaruh signifikan.
b. Sig. 0.000 < 0.05
    → Pengaruh sangat signifikan secara statistik.

3.6.5 Dampak Implementasi NGFW Berdasarkan Indikator

3.6.5.1 Deep Packet Inspection (DPI)

a. DPI memungkinkan firewall memeriksa isi paket hingga layer aplikasi.
b. KSBM dapat mendeteksi anomali seperti payload berbahaya, signature malware, dan exploit.
c. Data survei menunjukkan penurunan aktivitas mencurigakan hingga **30–40%**.

3.6.5.2 Intrusion Prevention System (IPS)

IPS KSBM mampu:

a. memblokir brute force login,
b. mendeteksi scanning port,
c. menghentikan serangan SQL injection dan cross-site scripting,
d. mengidentifikasi command-and-control server.

Kontribusi IPS terhadap keamanan sangat dominan dalam penelitian ini.

3.6.5.3 Web Filtering

NGFW dapat mengidentifikasi aplikasi berdasarkan signature, bukan sekadar port. KSBM memblokir aplikasi seperti:

a. torrent,
b. illegal proxy VPN,
c. remote access tool berbahaya.

Pengguna umum (mahasiswa) melaporkan kualitas koneksi yang lebih stabil setelah kontrol aplikasi diberlakukan.

3.6.5.4 SSL/HTTPS Inspection

Sebanyak 85% trafik internet Koperasi Sekolah Bina Mulia (KSBM) adalah terenkripsi. Sebelum NGFW:

malware tersembunyi dalam HTTPS sulit teridentifikasi.

Setelah NGFW:

a. malware dalam trafik terenkripsi dapat dideteksi,
b. phishing HTTPS dapat diblokir,
c. akses domain berbahaya langsung ditolak.

3.6.5.5 Threat Intelligence Update

NGFW KSBM menerima update signature otomatis setiap hari. Hasilnya:

a. deteksi ancaman zero-day lebih cepat,
b. respon terhadap malware baru meningkat signifikan,
c. false positive menurun.

3.7 Implikasi Penelitian

Penelitian ini menunjukkan bahwa NGFW merupakan komponen vital dalam infrastruktur keamanan modern koperasi sekolah.

Beberapa implikasi penting:

1. KSBM harus mempertahankan konfigurasi NGFW secara optimal.

2. Perlu ditambah dengan kebijakan Zero Trust dan segmentasi jaringan.
3. Pelatihan cybersecurity pengguna harus ditingkatkan.
4. Integrasi dengan SIEM akan memperkuat deteksi ancaman terpadu.

4. Kesimpulan

Penggunaan Firewall Generasi Terbaru (NGFW) berpengaruh positif dan signifikan terhadap tingkat keamanan jaringan di Koperasi Sekolah Bina Mulia. Hasil regresi membuktikan nilai R (0.812) dan R^2 (0.660), yang menunjukkan keberhasilan NGFW dalam meningkatkan keamanan jaringan hingga 66%. Fitur NGFW seperti DPI, IPS, Application Control, SSL Inspection, dan Threat Intelligence memberikan dampak besar terhadap penurunan ancaman dan peningkatan deteksi serangan. Implementasi NGFW harus diikuti dengan konfigurasi yang tepat, update signature, edukasi pengguna, dan kebijakan keamanan tambahan. KSBM disarankan mengembangkan sistem keamanan terpadu dengan konsep Zero Trust, segmentasi jaringan, dan monitoring berbasis SIEM agar keamanan lebih optimal. Implementasi Firewall Generasi Terbaru (NGFW) memiliki pengaruh positif dan signifikan terhadap tingkat keamanan jaringan di Koperasi Sekolah Bina Mulia. Fitur NGFW seperti DPI, IPS, Application Control, dan SSL inspection terbukti mampu menurunkan intensitas serangan siber, mendeteksi ancaman lebih cepat, serta meningkatkan stabilitas jaringan. Nilai R^2 (0.660) menunjukkan bahwa NGFW memberikan kontribusi besar (66%) dalam meningkatkan keamanan jaringan di koperasi sekolah. Meskipun demikian, penerapan NGFW harus disertai kebijakan keamanan lain seperti segmentasi jaringan, edukasi pengguna, dan monitoring berkala. KSBM dianjurkan untuk memperkuat integrasi NGFW dengan sistem keamanan lain seperti SIEM, endpoint security, dan Zero Trust Architecture untuk mencapai perlindungan optimal.

Daftar Pustaka

Adhi Purwaningrum, F., Purwanto, A., & Agus Darmadi, E. (2018). Optimalisasi Jaringan Menggunakan Firewall. *Jurnal IKRA-ITH Informatika*, *2*(3), 17–23.

Akbar, Y., Abdillah, G. P., Mulyana, D. I., & Sutisna. (2025). View of Optimization of Data Security Protection with Full SSL Inspection on AWS Using FortiGate Virtual Appliance.pdf. *International Journal Software Engineering and Computer Science (IJSECS)*, *5*(2), 887–896.

Anoname. (2023). IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs. In *IBM Newsroom*. https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs?

Bangun, A. M., Ferdian, E. D., & Safitri, A. M. (2025). IMPLEMENTASI FITUR TEMPORARY BLACKLIST PADA FIREWALL SANGFOR NGAF DALAM MITIGASI SERANGAN SIBER. *Jurnal Teknik*, *05*(03), 1708–1714.

Fitrian, H. P., Noorjamil, B. F., Rahmawati, F., & Rachman, S. A. (2025). Analisis Efektivitas Firewall dalam Memfilter dan Melindungi Lalu Lintas Jaringan. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *8*(1), 95–102. https://doi.org/10.32672/jnkti.v8i1.8554

Harja, D. P., Rakhmatsyah, A., & Nugroho, M. A. (2019). Implementasi untuk Meningkatkan Keamanan Jaringan Menggunakan Deep Packet Inspection pada Software Defined Networks. *Indonesian Journal on Computing (Indo-JC)*, *4*(1), 133.

https://doi.org/10.21108/indojc.2019.4.1.286

Haugerud, H., Tran, H. N., Aitsaadi, N., & Yazidi, A. (2021). A dynamic and scalable parallel Network Intrusion Detection System using intelligent rule ordering and Network Function Virtualization. *Future Generation Computer Systems*, *124*, 254–267. https://doi.org/10.1016/j.future.2021.05.037

Hore, S., Ghadermazi, J., Shah, A., & Bastian, N. D. (2024). A sequential deep learning framework for a robust and resilient network intrusion detection system. *Computers and Security*, *144*(June), 103928. https://doi.org/10.1016/j.cose.2024.103928

Khabib Adi Nugroho, Hariguna, T., & Barkah, A. S. (2025). Deteksi Anomali Trafik Jaringan dan Aktivitas Pengguna Menggunakan Isolation Forest untuk Meningkatkan Keamanan Jaringan. *Jurnal Pendidikan Dan Teknologi Indonesia*, *5*(5), 1365–1376. https://doi.org/10.52436/1.jpti.790

Miracle, N. O. (2023). *On the physical significance and di-electric response of Castor oil processed in Nigeria as transformer insulating fluid*. *VIII*(2454), 60–66. https://doi.org/10.51584/IJRIAS

Munira, Dasrilb, & Abduh, H. (2024). Jurnal Riset Sistem Informasi Membangun Web Filtering Dengan Dns Forwarding Pada Jaringan Wireless Berbasis Mikrotik Pada Sma Negeri 1 Palopo. *Denasya: Jurnal RIset Sistem Informasi*, *1*(3), 37–44.

Pratama, I. P. A. E., & Dharmesta, P. A. (2018). Implementasi Teknik Deep Packet Inspection Dengan Menggunakan Wireshark Pada Sistem Operasi Ubuntu (Studi Kasus : Intranet Jurusan Teknologi Informasi Universitas Udayana). *Jurnal Resistor*, *1*(2), 79–85. http://jurnal.stiki-indonesia.ac.id/index.php/jurnalresistor

Rivaldi, O., & Marpaung, N. L. (2023). Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata. *INOVTEK Polbeng - Seri Informatika*, *8*(1), 141. https://doi.org/10.35314/isi.v8i1.3269

Si-Ahmed, A., Al-Garadi, M. A., & Boustia, N. (2023). Survey of Machine Learning based intrusion detection methods for Internet of Medical Things. *Applied Soft Computing*, *140*, 0–2. https://doi.org/10.1016/j.asoc.2023.110227

Widyatono, D. P., & Sulistyo, W. (2023). Pemodelan Instrusion Prevention System Untuk Pendeteksi Dan Pencegahan Penyebaran Malware Menggunakan Wazuh. *Journal of Information Technology Ampera*, *4*(1), 113–127. https://journal-computing.org/index.php/journal-ita/index