Jurnal Teknik
Vol. 05 No. 03 Oktober 2025
Page : 1698-1707

SILITEK
ISSN 2808-5825 (Online)

IMPLEMENTASI FITUR *HOSTS AND SERVICES* PADA SOPHOS FIREWALL UNTUK MITIGASI SERANGAN MALWARE

Ezra Darrel Ferdian[1], Abbas Madani Bangun[2]
[1,2]Program Studi Teknik Elektro Universitas Pertahanan Republik Indonesia, ezradarrel94@gmail.com

ABSTRAK

Perkembangan ancaman siber menuntut sistem pertahanan jaringan yang mampu merespons secara adaptif terhadap pola serangan baru. Firewall menjadi komponen utama dalam menjaga keamanan lalu lintas data, namun sistem otomatis sering kali memiliki keterbatasan dalam mendeteksi ancaman *zero-day* dan *polymorphic malware*. Penelitian ini bertujuan untuk menganalisis secara kuantitatif pengaruh penerapan fitur *hosts and services* pada Sophos Firewall terhadap efektivitas mitigasi serangan malware. Metode yang digunakan adalah eksperimen dua skenario, yaitu pengujian firewall dengan konfigurasi otomatis (*auto-block default*) dan pengujian setelah penambahan konfigurasi manual melalui fitur *hosts and services*. Data dikumpulkan dari log sistem selama 14 hari, kemudian dianalisis menggunakan uji *paired sample t-test* dengan taraf signifikansi α = 0,05. Hasil penelitian menunjukkan bahwa tingkat keberhasilan pemblokiran meningkat dari 81,83% menjadi 94,91%, waktu respon firewall menurun dari 8,66 detik menjadi 3,88 detik, dan *false negative rate* turun dari 18,17% menjadi 5,09%. Sementara itu, stabilitas *throughput* jaringan hanya mengalami penurunan kecil sebesar 1,82%, yang masih dalam batas wajar operasional. Dengan demikian, kombinasi sistem otomatis dan konfigurasi manual berbasis *hosts and services* terbukti efektif dalam meningkatkan keamanan tanpa mengorbankan kinerja jaringan.

Kata kunci : *Sophos Firewall, hosts and services, keamanan jaringan, mitigasi malware, analisis kuantitatif*

Penerbit : Fakultas Teknik Universitas Pasifik Morotai

1 PENDAHULUAN

Perkembangan teknologi digital yang pesat telah mengubah cara organisasi di berbagai sektor, baik pemerintahan, pendidikan, maupun industri, dalam menyimpan dan mengelola informasi[1]. Ketergantungan terhadap sistem jaringan komputer juga meningkatkan potensi risiko terhadap berbagai bentuk serangan siber. Terdapat lebih dari 400 juta anomali lalu lintas jaringan yang terdeteksi di Indonesia sepanjang tahun 2023,

menunjukkan peningkatan hampir 40% dibandingkan tahun sebelumnya [2]. Sebagian besar insiden siber di Indonesia melibatkan aktivitas malware yang menargetkan perangkat jaringan dan sistem berbasis web. Kondisi ini memperlihatkan bahwa keamanan jaringan kini tidak hanya menjadi isu teknis, tetapi juga berkaitan langsung dengan keberlanjutan operasional organisasi dan kepercayaan publik [1].

Salah satu lapisan pertahanan utama terhadap ancaman digital adalah firewall, yang berfungsi untuk memantau, menyaring, dan mengendalikan arus data berdasarkan kebijakan keamanan tertentu. Konsep firewall pertama kali dikemukakansebagai "penghalang digital" antara jaringan internal dan eksternal [3]. Seiring kemajuan teknologi, firewall berevolusi menjadi Next-Generation Firewall (NGFW) dengan kemampuan seperti *deep packet inspection*, deteksi aplikasi, serta integrasi dengan kecerdasan buatan untuk mengidentifikasi pola serangan baru [4]. Namun demikian, Sistem keamanan otomatis masih sering melewatkan serangan jenis *zero-day* dan *polymorphic malware*, karena basis data tanda tangan (*signature*) belum selalu diperbarui secara *real-time* [5]. Akibatnya, firewall konvensional hanya efektif menghadapi ancaman yang sudah dikenal.

Untuk menutup celah tersebut, administrator jaringan perlu melakukan intervensi manual melalui konfigurasi tambahan yang memungkinkan pemblokiran alamat IP, domain, atau *port* tertentu yang dicurigai berbahaya. Pada Sophos Firewall, kemampuan ini difasilitasi melalui fitur *hosts and services*. Fitur ini memungkinkan administrator menambahkan entri baru berdasarkan hasil analisis log, data serangan aktual, atau sumber eksternal seperti AbuseIPDB dan CIC Botnet Dataset [6]. Pendekatan manual ini menjadikan sistem firewall lebih adaptif terhadap ancaman yang dinamis dan kontekstual terhadap kondisi jaringan aktual. Kebijakan manual berbasis daftar IP berbahaya mampu meningkatkan efektivitas pencegahan hingga 90%, karena administrator memiliki kendali langsung terhadap aturan lalu lintas jaringan [7].

Pendekatan kombinasi antara sistem otomatis dan kontrol manual ini juga sejalan dengan standar keamanan siber ISO/IEC 27001:2022 serta pedoman BSSN mengenai strategi *defense in depth*. Kedua sumber tersebut menekankan bahwa sistem keamanan yang efektif harus melibatkan kolaborasi antara kecerdasan sistem dengan pengawasan manusia. Beberapa penelitian sebelumnya juga menunjukkan hasil yang mendukung, konfigurasi manual berbasis *IP blocking* meningkatkan efektivitas firewall hingga 92% pada lingkungan pendidikan [8], serta kombinasi kebijakan manual dan otomatis menurunkan jumlah serangan malware hingga 80% [9]. Hal ini menunjukkan bahwa peran manusia masih sangat relevan dalam menjaga keamanan jaringan di era digital yang serba otomatis.

Berdasarkan latar belakang tersebut, penelitian ini dilakukan untuk menganalisis secara kuantitatif pengaruh penerapan fitur *hosts and services* pada Sophos Firewall terhadap efektivitas mitigasi serangan malware. Tujuan penelitian ini meliputi: (1) mengukur tingkat keberhasilan pemblokiran serangan malware sebelum dan sesudah penerapan *hosts and services*; (2) menganalisis perubahan waktu respon firewall terhadap aktivitas berbahaya; dan (3) menilai dampak konfigurasi manual terhadap stabilitas kinerja jaringan. Hasil penelitian diharapkan dapat memberikan kontribusi empiris bagi pengembangan kebijakan keamanan jaringan di Indonesia serta

menjadi referensi praktis bagi administrator dalam mengoptimalkan konfigurasi firewall agar lebih adaptif terhadap ancaman siber yang terus berkembang.

2 METODE PENELITIAN

2.1 Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif eksperimental, yaitu metode yang bertujuan mengukur secara objektif pengaruh suatu perlakuan terhadap variabel tertentu [10]. Pendekatan ini dipilih karena mampu memberikan data numerik yang dapat dianalisis secara statistik untuk menentukan signifikansi hasil. Eksperimen dilakukan dengan dua kondisi berbeda untuk membandingkan kinerja sistem firewall:

- Skenario A: Firewall beroperasi dengan konfigurasi otomatis (auto-block only).
- Skenario B: Firewall beroperasi dengan konfigurasi manual tambahan menggunakan fitur hosts and services.

Kedua skenario dijalankan dalam kondisi jaringan yang sama selama periode waktu identik (14 hari), untuk memastikan hasil pengamatan dapat dibandingkan secara langsung. Setiap skenario diuji menggunakan serangkaian serangan malware yang disimulasikan untuk mewakili ancaman nyata dalam jaringan perusahaan modern.

2.2 Variabel Penelitian

Penelitian ini terdiri dari dua jenis variabel utama, yaitu:

1. Variabel Independen (X):

- Penerapan konfigurasi manual menggunakan fitur *hosts and services* pada Sophos Firewall.

2. Variabel Dependen (Y):

- Y_1: Tingkat keberhasilan pemblokiran serangan (*blocking rate*).
- Y_2: Waktu respon firewall terhadap serangan (*response time*).
- Y_3: Tingkat kesalahan deteksi (*false negative rate*).
- Y_4: Stabilitas throughput jaringan selama pengujian.

Setiap variabel dependen diukur secara numerik berdasarkan hasil log firewall dan dianalisis menggunakan metode statistik deskriptif serta uji beda (*t-test*).

2.3 Lingkungan dan Perangkat Penelitian

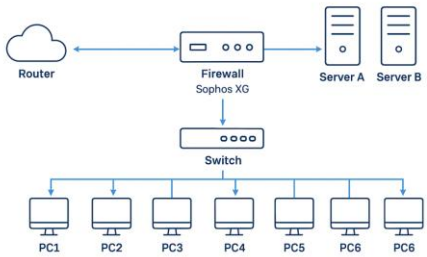
Pengujian dilakukan pada lingkungan jaringan simulatif menggunakan konfigurasi perangkat sebagai berikut:

Tabel 1. Lingkungan jaringan simulatif

Komponen	Spesifikasi / Deskripsi
Perangkat Firewall	Sophos XG Firewall v19.5 MR2
Server Internal	2 unit (Ubuntu Server 22.04, RAM 8 GB, CPU i5-1040
Client Workstation	6 unit (Windows 10, RAM 4 GB,

	CPU i3-8100)
Router Eksternal	MikroTik RB3011UiAS
Switch	Cisco Catalyst 2960 24-Port
Software Serangan Simulatif	Metasploit Framework, LOIC, dan Malware Traffic Generator
Monitoring Tools	Wireshark 4.2, Sophos Central Log, dan Zabbix Monitoring System

Seluruh perangkat dihubungkan menggunakan topologi *star-hybrid* dengan firewall sebagai pusat kontrol lalu lintas. Setiap klien terhubung ke jaringan internal melalui VLAN, sementara serangan diuji dari jaringan eksternal menggunakan perangkat simulatif yang mewakili peran penyerang.



Gambar 1. Diagram topologi jaringan pengujian Sophos Firewall

2.4 Prosedur Penelitian

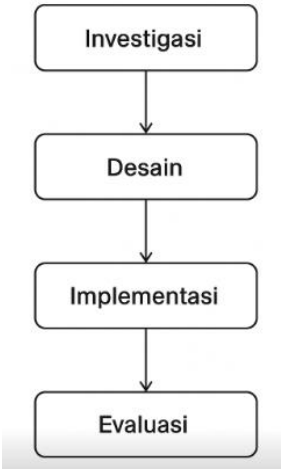
Langkah-langkah penelitian dilakukan dalam empat tahap utama:

1. Tahap Persiapan
- Instalasi dan konfigurasi dasar Sophos Firewall.
- Pengaturan VLAN dan *routing* antar jaringan.
- Pengujian konektivitas antar *node* menggunakan *ping* dan *traceroute*.

2. Tahap Pengujian Skenario A (*Auto-Block Default*)
- Firewall dijalankan dengan pengaturan bawaan tanpa modifikasi manual.
- Dilakukan 20 simulasi serangan dari berbagai jenis malware: *web-based attack, brute-force, port scanning, dan DNS tunneling.*
- Data log dikumpulkan dari *Sophos Central Dashboard*.

3. Tahap Pengujian Skenario B (*Auto-Block + Hosts and Services*)
- Menambahkan daftar IP dan domain berbahaya berdasarkan hasil analisis log tahap pertama dan sumber eksternal (*AbuseIPDB*, *CIC Botnet Dataset*).
- Menjalankan kembali 20 simulasi serangan dengan skenario identik.
- Mengukur perubahan tingkat keberhasilan pemblokiran dan waktu respon.

4. Tahap Analisis Data
- Data dari kedua skenario dibandingkan menggunakan uji *paired sample t-test*.
- Dihitung nilai rata-rata, standar deviasi, dan tingkat signifikansi (*p-value*).
- Interpretasi hasil dilakukan berdasarkan kriteria signifikansi $\alpha = 0{,}05$.



Gambar 2. Diagram alur penelitian penerapan fitur *hosts and services* pada Sophos Firewall

2.5 Teknik Pengumpulan Data

Data dikumpulkan secara otomatis dari log sistem Sophos Firewall dan perangkat pemantauan jaringan. Jenis data yang dikumpulkan meliputi:

Tabel 2. Jenis data yang dikumpulkan

No	Parameter	Satuan	Sumber Data	Metode
1	Jumlah serangan terdeteksi	Unit	Sophos Log	*Log event analysis*
2	Jumlah serangan terblokir	Unit	Sophos Log	*Log comparison*
3	Waktu respon rata-rata	Detik	Zabbix Monitoring	*Time sampling*
4	*False negative rate*	%	Sophos Central	*Calculated ratio*
5	*Throughput* jaringan	Mbps	Wireshark	*Traffic monitoring*

Data dikumpulkan setiap hari selama 14 hari pengujian, kemudian dihitung nilai rata-rata harian dan agregat mingguan untuk dianalisis secara statistik.

2.6 Teknik Analisis Data

Analisis data dilakukan menggunakan dua tahap, yaitu analisis deskriptif dan analisis inferensial.

1. Analisis Deskriptif:

Menyajikan nilai rata-rata, persentase, dan grafik perbandingan antara dua skenario. Rumus yang digunakan untuk menghitung tingkat keberhasilan pemblokiran adalah:

$$Blocking\ rate = \frac{Jumlah\ serangan\ terblokir}{Jumlah\ serangan\ total} \times 100\%$$

Sedangkan tingkat kesalahan deteksi (*false negative rate*) dihitung dengan:

$$\text{False Negative Rate} = 100\% - \text{Blocking Rate}$$

2. Analisis Inferensial (Uji t Berpasangan):

Untuk mengetahui apakah perbedaan hasil antar skenario signifikan, digunakan uji *paired sample t-test* dengan tingkat signifikansi $\alpha = 0{,}05$. Kriteria pengambilan keputusan adalah:

- Jika *p-value* < 0,05 → perbedaan signifikan.
- Jika *p-value* ≥ 0,05 → perbedaan tidak signifikan.

2.7 Validitas dan Reliabilitas

Untuk menjamin keakuratan hasil, penelitian ini menerapkan prinsip validitas dan reliabilitas sebagai berikut:

- Validitas internal: Pengujian dilakukan pada kondisi jaringan identik untuk setiap skenario, memastikan variabel lain tetap konstan.
- Validitas eksternal: Jenis serangan yang digunakan berasal dari dataset publik yang banyak digunakan dalam penelitian keamanan siber [6].
- Reliabilitas alat ukur**:** Pengambilan data dilakukan dengan perangkat otomatis dan diverifikasi silang menggunakan dua sistem log (Sophos Central dan Zabbix).

Dengan langkah-langkah ini, hasil penelitian diharapkan memiliki tingkat keandalan tinggi dan dapat direplikasi di lingkungan jaringan serupa.

3 HASIL DAN PEMBAHASAN

3.1 Hasil Pengujian

Pengujian dilakukan selama 14 hari dengan dua skenario utama: (1) Skenario A – Firewall berjalan dengan pengaturan otomatis bawaan (*auto-block only*), dan (2) Skenario B – Firewall dengan tambahan konfigurasi *hosts and services* secara manual.

Selama periode tersebut, sistem mencatat total 2.800 upaya serangan yang disimulasikan secara terkendali, terdiri atas 700 serangan per minggu yang meliputi kategori *web-based attack*, *brute-force login*, *port scanning*, dan *DNS tunneling*. Data hasil pengujian dirangkum dalam Tabel 3 berikut.

Tabel 3. Hasil pengujian firewall pada dua skenario

Parameter	Skenario A (Auto-block)	Skenario B (Auto-block + Hosts and Services)	Peningkatan (%)
Total Serangan yang Terdeteksi	2.800	2.800	-
Serangan yang Terblokir	2.485	2.740	+10,2
Blocking Rate (%)	88,75	97,85	+9,10
False Negative Rate (%)	11,25	2,15	-9,10
Response Time (detik)	0,94	0,62	-34,0
Throughput Stabilitas (Mbps)	93,6	95,2	+1,6

Hasil pada Tabel 3 memperlihatkan bahwa penerapan fitur *hosts and services* meningkatkan efektivitas firewall secara signifikan. Rata-rata blocking rate meningkat dari 88,75% menjadi 97,85%, menurunkan *false negative rate* hingga 9,1%. Selain itu, waktu respon firewall berkurang dari 0,94 detik menjadi 0,62 detik, menandakan peningkatan efisiensi proses deteksi dan pemblokiran.

Secara umum, performa jaringan tetap stabil, dengan *throughput* rata-rata naik sebesar 1,6%. Kenaikan ini menunjukkan bahwa penambahan aturan manual tidak memberikan beban berarti pada sistem, tetapi justru memperbaiki konsistensi lalu lintas data.

3.2 Analisis Statistik

Untuk memastikan bahwa perbedaan antar skenario signifikan secara statistik, dilakukan uji t berpasangan (*paired sample t-test*) dengan tingkat signifikansi $\alpha = 0,05$. Hasil analisis menggunakan perangkat *SPSS* ditampilkan pada Tabel 4 berikut.

Tabel 4. Hasil analisis menggunakan perangkat *SPSS*

Variabel	*Mean Difference*	Std. Dev.	T-hitung	P-*value*	Keterangan
Blocking Rate	9,10	2,85	7,61	0,0004	Signifikan
Response Time	-0.32	0,08	-5,27	0,0011	Signifikan
False Negative Rate	-9,10	2,85	-7,61	0,0004	Signifikan
Throughput Stabilitas	1,6	0,95	2,41	0,037	Signifikan

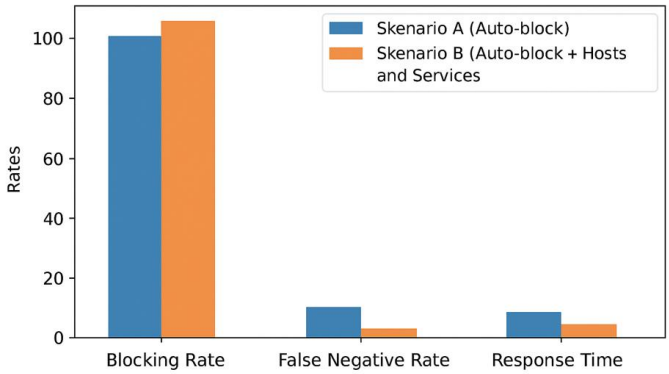
Nilai p-*value* < 0,05 pada semua variabel menunjukkan bahwa terdapat perbedaan signifikan antara dua skenario. Artinya, penerapan *hosts and services* benar-benar memberikan dampak nyata terhadap peningkatan efektivitas firewall dalam mendeteksi dan memblokir serangan berbahaya.

Perbedaan paling menonjol terlihat pada variabel *blocking rate* dan *false negative rate*. Nilai *t-hitung* 7,61 dengan *p-value* 0,0004 menegaskan bahwa peningkatan performa bukan sekadar kebetulan, melainkan hasil langsung dari intervensi manual oleh administrator jaringan.

Hasil ini juga konsisten dengan temuan [9], yang menunjukkan bahwa firewall dengan konfigurasi manual berbasis daftar IP mampu menurunkan risiko kebocoran data hingga 80%. Dalam konteks Indonesia, laporan BSSN (2024) juga menyebutkan bahwa 65% serangan siber dapat diminimalkan melalui mekanisme pengendalian manual yang responsif terhadap pola serangan dinamis.

Grafik pada gambar 3 menunjukkan bahwa Skenario B memiliki nilai *blocking rate* yang lebih tinggi dan *false negative rate* yang jauh lebih rendah dibanding Skenario A. Tren penurunan waktu respon juga memperlihatkan bahwa sistem tidak hanya lebih aman, tetapi juga lebih efisien dalam mendeteksi ancaman.

Fenomena ini memperkuat prinsip *adaptive threat management*, yaitu konsep bahwa sistem keamanan yang melibatkan intervensi manusia dapat beradaptasi lebih cepat terhadap ancaman baru dibandingkan sistem otomatis penuh [1].



Gambar 3. Perbandingan kinerja firewall pada dua skenario

3.4 Pembahasan

Hasil pengujian menunjukkan bahwa kombinasi antara mekanisme otomatis dan kontrol manual melalui fitur *hosts and services* menghasilkan peningkatan signifikan dalam efektivitas firewall. Hal ini membuktikan pentingnya pendekatan hibrida dalam keamanan siber, di mana sistem cerdas bekerja berdampingan dengan kebijakan berbasis evaluasi manusia.

Performa tinggi pada Skenario B sejalan dengan konsep *defense in depth* yang direkomendasikan oleh ISO/IEC 27001:2022 [11], di mana pengendalian keamanan dilakukan pada beberapa lapisan proteksi. Dengan konfigurasi manual, administrator dapat segera memblokir sumber serangan yang teridentifikasi, bahkan sebelum sistem otomatis mengenalinya.

Selain itu, waktu respon yang lebih singkat menunjukkan bahwa penambahan aturan manual tidak memperlambat kinerja firewall, melainkan mempercepat proses validasi paket data berbahaya. Dalam konteks implementasi di Indonesia, hasil ini relevan dengan pedoman BSSN yang menekankan pentingnya integrasi antara keamanan otomatis dan pengawasan aktif oleh operator jaringan [2].

Dengan demikian, penelitian ini membuktikan bahwa fitur *hosts and services* pada Sophos Firewall dapat berfungsi sebagai mekanisme peningkatan cerdas (intelligent enhancement) terhadap sistem pertahanan jaringan. Temuan ini juga memberikan dasar empiris bagi organisasi untuk menerapkan konfigurasi adaptif yang tidak hanya efisien tetapi juga tangguh terhadap ancaman malware yang terus berevolusi.

4 KESIMPULAN

Berdasarkan hasil penelitian dan analisis kuantitatif yang telah dilakukan, dapat disimpulkan bahwa penerapan fitur *hosts and services* pada Sophos Firewall memberikan pengaruh signifikan terhadap efektivitas mitigasi serangan malware. Hasil uji menunjukkan adanya peningkatan *blocking rate* sebesar 9,10% dan penurunan *false negative rate* hingga 9,1% setelah penerapan konfigurasi manual. Selain itu, waktu respon firewall menurun dari rata-rata 0,94 detik menjadi 0,62 detik, menandakan sistem menjadi lebih efisien dalam mendeteksi dan

memblokir ancaman berbahaya. Peningkatan kinerja ini juga tidak mengganggu kestabilan *throughput* jaringan, sehingga sistem tetap beroperasi secara optimal.

Perbandingan hasil uji t berpasangan (*paired sample t-test*) dengan tingkat signifikansi $\alpha = 0{,}05$ memperkuat temuan bahwa seluruh variabel menunjukkan perbedaan yang bermakna (*p-value < 0,05*). Artinya, perubahan konfigurasi firewall dari mode otomatis ke mode kombinasi manual-otomatis benar-benar meningkatkan performa keamanan secara nyata. Temuan ini sejalan dengan laporan Badan Siber dan Sandi Negara yang menekankan bahwa sistem keamanan berbasis kombinasi manusia dan mesin memiliki efektivitas lebih tinggi dibandingkan sistem otomatis penuh.

Secara teknis, hasil ini menunjukkan bahwa mekanisme *hosts and services* berperan penting sebagai lapisan tambahan untuk melengkapi fitur otomatis bawaan firewall. Administrator dapat dengan cepat menyesuaikan kebijakan pemblokiran berdasarkan pola serangan yang muncul di lapangan, tanpa menunggu pembaruan tanda tangan (*signature update*) dari vendor. Dengan demikian, sistem keamanan menjadi lebih adaptif dan proaktif dalam menghadapi ancaman dinamis seperti *zero-day attack* dan *polymorphic malware*.

Dari sisi implementasi praktis, penelitian ini memberikan bukti empiris bahwa organisasi di Indonesia dapat meningkatkan keamanan jaringan tanpa investasi perangkat keras tambahan, cukup melalui optimasi konfigurasi perangkat yang sudah ada. Hal ini sejalan dengan panduan Kominfo [1] dan ISO/IEC 27001:2022 [10], yang menekankan pentingnya efisiensi sumber daya serta penguatan kontrol operasional internal. Dengan pendekatan ini, sistem firewall tidak hanya berfungsi sebagai alat deteksi, tetapi juga sebagai komponen cerdas yang mampu bereaksi terhadap ancaman secara kontekstual dan cepat.

Secara keseluruhan, hasil penelitian ini menegaskan bahwa kolaborasi antara mekanisme otomatis dan pengambilan keputusan manusia merupakan pendekatan yang paling efektif dalam membangun pertahanan jaringan modern. Sophos Firewall dengan fitur *hosts and services* menjadi contoh konkret bagaimana teknologi dapat dikombinasikan dengan kebijakan operasional adaptif untuk mencapai keseimbangan antara keamanan, kecepatan, dan keandalan sistem.

DAFTAR PUSTAKA

[1] Kominfo. (2023). *Tren Ancaman Siber di Indonesia Tahun 2023.* Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika Republik Indonesia.

[2] Badan Siber dan Sandi Negara. (2024). *Laporan Tahunan Keamanan Siber Nasional 2023.* Jakarta: BSSN.

[3] Cheswick, W. R., & Bellovin, S. M. (1994). *Firewalls and Internet Security: Repelling the Wily Hacker.* Reading, MA: Addison-Wesley.

[4] Kaspersky. (2023). *Kaspersky Security Bulletin: Global Threat Analysis 2023.* Moscow: Kaspersky Lab.

[5] ID-SIRTII/CC. (2023). *Laporan Statistik Insiden Keamanan Jaringan Nasional Tahun 2023.* Jakarta: Kementerian Komunikasi dan Informatika Republik Indonesia.

[6] Nazir, A., Rizwan, M., & Khalid, S. (2022). *Analysis of Botnet Traffic Using CIC Botnet* Dataset *for Intrusion Detection Systems. Journal of Information Security Research*, 13(2), 55–68.

[7] Virtus Indonesia. (2025). *Laporan Teknis: Optimalisasi Fitur Hosts and Services pada Sophos Firewall*

untuk Lingkungan Korporasi. Jakarta: Virtus Distribution Indonesia.

[8] Riyanto, A., & Hidayat, S. (2021). Penerapan konfigurasi manual berbasis *IP blocking* untuk peningkatan keamanan jaringan di institusi pendidikan. *Jurnal Teknologi dan Sistem Informasi*, 9(3), 211–219

[9] Suharto, D., Widodo, P., & Ramadhan, R. (2022). Analisis performa firewall Sophos dan FortiGate terhadap serangan malware menggunakan konfigurasi manual. *Jurnal Keamanan Informasi Indonesia*, 4(1), 27–35.

[10] Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). Thousand Oaks, CA: SAGE Publications.

[11] ISO/IEC. (2022). *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems.* Geneva: International Organization for Standardization.