JIKUM
JURNAL ILMU KOMPUTER

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

Implementasi Keamanan Jaringan Menggunakan Firewall dan Intrusion Detection System (IDS) pada Infrastruktur Jaringan Skala Kecil–Menengah

Ferdi Ardiansyah sihombing[1], Naila Nafisa Zuhra[2*], Lia Zahra[3], Rahul Alfarisyi[4], Hidayatun Nisa[5], Rafi Alfarsi Astiyanto[6]
[1,2,3,4,5, 6]Universitas Malikussaleh, Indonesia
[1] ferdi.240170004@mhs.unimal.ac.id, [2] naila.240170006@mhs.unimal.ac.id, [3] lia.240170007@mhs.unimal.ac.id, [4]rahul.240170009@mhs.unimal.ac.id, [5]hidayatun.240170014@mhs.unimal.ac.id, [6]rafi.240170022@mhs.unimal.ac.id

ABSTRACT

Network security plays a vital role in ensuring the confidentiality, integrity, and availability of data in small- to medium-scale network infrastructures. This study aims to implement and evaluate the effectiveness of a layered network security system using a Firewall and an Intrusion Detection System (IDS). The methods employed include system design, firewall rule configuration using iptables and pfSense, deployment of IDS Snort/Suricata, traffic monitoring, and performance evaluation. The testing scenarios involve normal traffic, port scanning, brute force attempts, and simulated Distributed Denial of Service (DDoS) attacks. The results indicate that the implementation of firewall and IDS significantly enhances network protection by filtering malicious traffic, improving attack detection accuracy, and maintaining network stability. These findings suggest that the integration of firewall and IDS provides an optimal and efficient security solution for small- to medium-scale network environments.

Keywords: *Firewall, IDS, Keamanan Jaringan, Penyaringan Paket, Deteksi Intrusi*

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong peningkatan penggunaan jaringan komputer sebagai media utama dalam pertukaran data dan informasi. Pemanfaatan jaringan komputer yang semakin luas pada institusi pendidikan, instansi pemerintahan, serta perusahaan skala kecil dan menengah diikuti dengan meningkatnya risiko ancaman keamanan jaringan. Ancaman tersebut meliputi serangan Distributed Denial of Service (DDoS), port scanning, malware injection, serta eksploitasi celah keamanan yang dapat mengganggu ketersediaan, kerahasiaan, dan integritas data (Stallings, 2017). Perkembangan serangan jaringan yang semakin kompleks juga menuntut sistem keamanan untuk mampu mendeteksi pola serangan secara adaptif dan real-time, terutama pada lingkungan jaringan modern (Zarpelão et al., 2020).

Jaringan berskala kecil hingga menengah cenderung memiliki tingkat kerentanan yang lebih tinggi akibat keterbatasan sumber daya keamanan, baik dari sisi perangkat, tenaga ahli, maupun kebijakan pengamanan yang diterapkan. Oleh karena itu, diperlukan mekanisme keamanan jaringan yang mampu memberikan perlindungan secara efektif dan berlapis. keamanan jaringan merupakan bagian penting dari keamanan siber yang harus diperhatikan oleh organisasi skala kecil dan menengah (Behl, 2018).

Firewall merupakan salah satu sistem keamanan jaringan yang berfungsi untuk mengontrol lalu lintas jaringan dengan melakukan pemfilteran paket berdasarkan aturan tertentu (Cheswick, Bellovin, & Rubin, 2003). Namun, firewall memiliki keterbatasan dalam mendeteksi serangan yang bersifat kompleks dan tidak terdefinisi secara eksplisit dalam aturan. Untuk mengatasi keterbatasan tersebut, Intrusion Detection System (IDS) digunakan sebagai sistem pendeteksi aktivitas mencurigakan atau upaya penyusupan ke dalam jaringan.

Integrasi antara firewall dan IDS telah banyak digunakan untuk meningkatkan efektivitas keamanan jaringan dengan mengombinasikan mekanisme pencegahan dan pendeteksian serangan (Alqahtani et al., 2021). Firewall berperan sebagai lapisan awal dalam membatasi akses yang tidak sah, sementara IDS berfungsi untuk memantau dan menganalisis aktivitas jaringan guna mendeteksi potensi serangan. Penelitian ini bertujuan untuk merancang sistem keamanan jaringan menggunakan firewall dan IDS pada jaringan skala kecil-menengah, menganalisis efektivitas konfigurasi firewall dalam memfilter lalu lintas berbahaya, serta mengukur kemampuan IDS dalam mendeteksi aktivitas penyusupan ke dalam jaringan melalui analisis pola lalu lintas jaringan (Scarfone & Mell, 2007).

KAJIAN LITERATUR

Firewall dapat didefinisikan sebagai sistem keamanan jaringan yang digunakan untuk mengatur dan membatasi lalu lintas data sesuai dengan kebijakan keamanan yang telah ditentukan (Cheswick, Bellovin, & Rubin, 2003). Perkembangan teknologi firewall menghasilkan Next Generation Firewall (NGFW) yang dilengkapi dengan kemampuan Deep Packet Inspection (DPI) untuk meningkatkan efektivitas deteksi dan penyaringan lalu lintas jaringan

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

(Zhang et al., 2019).

Intrusion Detection System (IDS) merupakan sistem keamanan yang dirancang untuk mendeteksi aktivitas mencurigakan atau berbahaya yang terjadi pada jaringan maupun host (Scarfone & Mell, 2007). Berdasarkan cakupannya, IDS dibagi menjadi Network-based Intrusion Detection System (NIDS) dan Host-based Intrusion Detection System (HIDS). Salah satu perangkat IDS yang banyak digunakan adalah Snort, yaitu sistem deteksi intrusi berbasis signature yang bersifat open source dan mampu mendeteksi berbagai pola serangan jaringan (Roesch, 1999). Meskipun IDS mampu mendeteksi berbagai pola serangan, efektivitasnya sangat bergantung pada kualitas data dan metode deteksi yang digunakan, sehingga masih memiliki keterbatasan dalam menghadapi serangan baru yang bersifat kompleks (Sommer & Paxson, 2020).

Beberapa penelitian terdahulu mengindikasikan bahwa penerapan firewall dan IDS secara bersamaan mampu memperkuat sistem keamanan jaringan. Salah satu pendekatan yang banyak digunakan adalah penerapan teknik data mining dan machine learning, yang terbukti mampu meningkatkan akurasi deteksi serangan dibandingkan metode konvensional berbasis signature (Buczak & Guven, 2020). Studi pada lingkungan enterprise menunjukkan bahwa Intrusion Detection System (IDS) efektif dalam mendeteksi berbagai jenis serangan secara real-time dan dapat meningkatkan tingkat keamanan sistem jaringan, sementara firewall berperan sebagai mekanisme pencegahan awal terhadap lalu lintas berbahaya (Sharma & Sahay, 2016; Bhuyan, Bhattacharyya, & Kalita, 2014). Kajian empiris lainnya juga menyebutkan bahwa integrasi antara firewall dan IDS dapat menurunkan risiko ancaman terhadap jaringan dengan biaya implementasi yang relatif minimal.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimen untuk menguji efektivitas penerapan firewall dan Intrusion Detection System (IDS) dalam meningkatkan keamanan jaringan skala kecil–menengah. Eksperimen dilakukan dengan membangun lingkungan jaringan uji yang menyerupai kondisi jaringan nyata.

Rancangan sistem menggunakan topologi jaringan yang terdiri dari satu router, satu firewall, satu server IDS, satu server layanan, dan beberapa client. Firewall yang digunakan adalah pfSense atau iptables, sedangkan IDS yang diterapkan adalah Snort atau Suricata. Objek penelitian berupa jaringan laboratorium yang mensimulasikan jaringan skala kecil–menengah dengan jumlah client sebanyak 20–30 perangkat. Perangkat dan perangkat lunak yang digunakan meliputi laptop atau PC server, router, switch, pfSense atau iptables, Snort atau Suricata, Wireshark, serta Kali Linux sebagai alat untuk melakukan pengujian serangan.

Pengumpulan data dilakukan melalui monitoring lalu lintas jaringan, analisis log firewall, analisis log IDS, serta pencatatan hasil pengujian serangan. Pengujian sistem dilakukan dengan beberapa skenario, yaitu lalu lintas normal, port scanning menggunakan Nmap, serangan brute force, dan simulasi serangan DDoS ringan. Monitoring lalu lintas jaringan dilakukan untuk membedakan antara trafik normal dan trafik mencurigakan sebagai bagian dari evaluasi keamanan jaringan (Sanders, 2015). Analisis data dilakukan dengan mengevaluasi tingkat keberhasilan firewall dalam memblokir lalu lintas berbahaya, kemampuan IDS dalam mendeteksi aktivitas penyusupan, serta dampak penerapan sistem keamanan terhadap performa jaringan.

HASIL DAN PEMBAHASAN

Berdasarkan hasil implementasi yang telah dilakukan, sistem keamanan jaringan menggunakan firewall dan Intrusion Detection System (IDS) berhasil diterapkan sesuai dengan rancangan yang telah ditentukan. Firewall dikonfigurasi dengan sejumlah aturan dasar (rules) untuk meningkatkan keamanan jaringan, antara lain memblokir lalu lintas jaringan yang tidak dikenal, membatasi akses pada port-port tertentu yang berpotensi disalahgunakan, serta mengizinkan lalu lintas internal yang sah sesuai dengan kebutuhan jaringan.

IDS yang digunakan dalam penelitian ini mampu mendeteksi berbagai aktivitas jaringan yang mencurigakan. Hasil pengujian menunjukkan bahwa IDS berhasil mengidentifikasi serangan port scanning dan brute force melalui pola lalu lintas yang tidak normal, serta memberikan peringatan (alert) secara real-time kepada administrator jaringan.

Hasil pengujian sistem keamanan jaringan terhadap beberapa skenario serangan ditunjukkan pada Tabel 1.

Tabel 1. Hasil Pengujian Sistem Keamanan Jaringan

Jenis Serangan	Terdeteksi IDS	Diblokir Firewall	Status Jaringan
Port Scanning	Ya	Ya	Aman
Brute Force	Ya	Ya	Aman
DDoS Ringan	Ya	Sebagian	Stabil

Pembahasan

Berdasarkan Tabel 1, dapat diketahui bahwa integrasi firewall dan IDS mampu memberikan perlindungan yang efektif terhadap sebagian besar serangan yang diuji. Serangan port scanning dan brute force dapat dideteksi oleh IDS

JIKUM
JURNAL ILMU KOMPUTER

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

dan diblokir sepenuhnya oleh firewall, sehingga tidak berdampak terhadap kestabilan jaringan.

Pada simulasi serangan DDoS ringan, IDS berhasil mendeteksi adanya peningkatan trafik yang tidak normal, sementara firewall mampu membatasi sebagian trafik berbahaya. Meskipun tidak seluruh trafik DDoS dapat diblokir, kondisi jaringan tetap berada dalam keadaan stabil dan masih dapat digunakan. Hal ini menunjukkan bahwa kombinasi firewall dan IDS mampu meningkatkan ketahanan jaringan terhadap serangan, meskipun diperlukan konfigurasi lanjutan untuk menghadapi serangan berskala lebih besar. Hasil pengujian sistem IDS pada penelitian ini sejalan dengan studi sebelumnya yang menyatakan bahwa IDS mampu meningkatkan kemampuan deteksi serangan tanpa menurunkan performa jaringan secara signifikan apabila dikonfigurasi dengan tepat (Mishra et al., 2022).

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa implementasi firewall dan Intrusion Detection System (IDS) pada jaringan skala kecil–menengah mampu meningkatkan tingkat keamanan jaringan secara signifikan. Firewall berperan efektif dalam memfilter dan membatasi lalu lintas jaringan yang berpotensi berbahaya, sedangkan IDS mampu mendeteksi aktivitas mencurigakan serta berbagai bentuk serangan secara dini.

Hasil pengujian menunjukkan bahwa sebagian besar serangan, seperti port scanning dan brute force, dapat dideteksi dan diblokir dengan baik tanpa mengganggu kestabilan jaringan. Pada simulasi serangan DDoS ringan, sistem keamanan yang diterapkan masih mampu menjaga performa jaringan tetap stabil meskipun tidak seluruh trafik berbahaya dapat diblokir sepenuhnya.

Sebagai pengembangan ke depan, penelitian selanjutnya disarankan untuk mengintegrasikan sistem dengan Intrusion Prevention System (IPS) guna meningkatkan kemampuan pencegahan serangan secara otomatis. Selain itu, pengujian pada skala jaringan yang lebih besar dan dengan variasi serangan yang lebih kompleks juga perlu dilakukan untuk memperoleh hasil yang lebih komprehensif.

REFERENSI

Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). Firewalls and Internet Security: Repelling the Wily Hacker. Addison Wesley.

Stallings, W. (2017). Network Security Essentials. Pearson.

Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication.

Sharma, A., & Sahay, S. (2016). A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and MANETs. Journal of Network and Computer Applications.

Roesch, M. (1999). Snort – Lightweight Intrusion Detection for Networks. USENIX.

Sanders, C. (2015). Practical Packet Analysis. No Starch Press.

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network Anomaly Detection: Methods, Systems and Tools. IEEE Communications Surveys and Tutorials.

Behl, R. (2018). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford.

Zhang, Y., et al. (2019). Next-Generation Firewall Technologies. IEEE Access.

Almubairik, A. (2020). Performance Analysis of IDS in Enterprise Networks. Journal of Network Security.

Sommer, R., & Paxson, V. (2020). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.

Buczak, A. L., & Guven, E. (2020). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2020). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25–37.

Alqahtani, S., Alshamrani, A., & Alshehri, M. (2021). Network security enhancement using integrated firewall and intrusion detection system. International Journal of Advanced Computer Science and Applications, 12(3), 432–438.

Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. S. (2022). A detailed investigation and analysis of using machine learning techniques for intrusion detection. IEEE Communications Surveys & Tutorials, 21(1), 686–728.