JIKUM
JURNAL ILMU KOMPUTER

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

Analisis Efektivitas Kebijakan Manajemen User dan Firewall pada Sistem Operasi dalam Mencegah Akses Ilegal

Anisah[1], Cut Intan Efrina[2], Muhammad Lukmanul Hakim[3], Nadhirah Adzra Afifah Siregar[4*], Yusra Putri Maulida[5]
[1,2,3,4,5]Program Studi Teknik Informatika Universitas Malikussaleh,Indonesia
Jl. Kampus Unimal Bukit Indah, Blang Pulo, Kec. Muara Satu, Kota Lhokseumawe, Aceh 24355 email:
anisah.240170040@mhs.unimal.ac.id[1], cut.240180062@mhs.unimal.ac.id[2], muhammad.240180061@mhs.unimal.ac.id[3], nadhirah.240170034@mhs.unimal.ac.id[4], yusra.240180023@mhs.unimal.ac.id[5]

ABSTRACT

Information system security is a crucial aspect in managing modern operating systems as the threat of unauthorized access to information systems increases. Therefore, effective protection strategies such as user access management policies and firewall implementation are needed in operating systems. This study aims to analyze the effectiveness of user management and firewall policies in preventing unauthorized access to operating systems by comparing their implementations in Windows and Linux. The method used in this study is a qualitative approach through literature studies of various relevant research and case studies. The findings show that user management plays a role in controlling internal access rights by implementing the principle of least privilege, while firewalls function as an effective external defense layer in controlling network traffic. Both complement each other in maintaining system security. However, their success is highly dependent on the implementation of stable rules, accurate settings, and the competence of system administrators. By combining good policies and proper firewall configuration, operating systems can be more robust against various unauthorized access risks, thus maintaining data and infrastructure security.

Kata Kunci: *Operating System Security, Firewall, User Management, Illegal Access.*

PENDAHULUAN

Keamanan sistem informasi merupakan aspek krusial dalam pengelolaan sistem operasi modern seiring meningkatnya ketergantungan organisasi terhadap teknologi digital. Sistem operasi berperan sebagai pengendali utama sumber daya perangkat keras dan perangkat lunak, sehingga menjadi target utama berbagai bentuk serangan siber, khususnya akses ilegal yang dapat mengancam kerahasiaan, integritas, dan ketersediaan data. Laporan keamanan siber dalam beberapa tahun terakhir menunjukkan peningkatan signifikan terhadap insiden akses tidak sah yang disebabkan oleh lemahnya kontrol akses dan pengamanan jaringan [1].

Salah satu mekanisme utama dalam menjaga keamanan sistem operasi adalah penerapan kebijakan manajemen user. Manajemen user meliputi pengaturan akun pengguna, autentikasi, otorisasi, serta pembatasan hak akses berdasarkan prinsip least privilege [2]. Kebijakan ini bertujuan untuk memastikan bahwa setiap pengguna hanya memiliki akses sesuai dengan kebutuhan dan tanggung jawabnya. Penelitian terkini menunjukkan bahwa kesalahan konfigurasi akun pengguna dan lemahnya pengawasan hak akses menjadi faktor dominan terjadinya pelanggaran keamanan internal.

Selain manajemen user, firewall berperan penting dalam melindungi sistem operasi dari ancaman eksternal. Firewall berfungsi sebagai mekanisme penyaringan lalu lintas jaringan dengan menerapkan aturan keamanan tertentu untuk mengontrol data yang masuk dan keluar dari sistem. Implementasi firewall yang efektif dapat mencegah serangan seperti *unauthorized access*, *port scanning*, dan penyebaran malware. Namun, efektivitas firewall sangat dipengaruhi oleh kebijakan konfigurasi dan integrasinya dengan sistem operasi.

Meskipun berbagai kebijakan keamanan telah diterapkan, masih banyak sistem operasi yang rentan terhadap akses ilegal akibat kurang optimalnya penerapan manajemen user dan firewall. Beberapa studi terbaru menekankan bahwa keberhasilan pencegahan akses ilegal tidak hanya bergantung pada keberadaan mekanisme keamanan, tetapi juga pada konsistensi kebijakan, pemantauan berkelanjutan, serta pemahaman administrator sistem terhadap risiko keamanan.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis efektivitas kebijakan manajemen user dan firewall pada sistem operasi dalam mencegah akses ilegal. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan pemahaman mengenai penerapan kebijakan keamanan sistem operasi yang lebih efektif dan berkelanjutan.

JIKUM
JURNAL ILMU KOMPUTER

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

KAJIAN LITERATUR

Keamanan Sistem Operasi

Aspek paling penting dari Keamanan Sistem Informasi adalah menjaga kerahasiaan, keutuhan, dan ketersediaan sistem. Sistem operasi adalah garda terdepan dalam pertahanan. Ragam ancaman terhadap sistem yang bisa menyebabkan masuk tanpa izin semakin banyak, mulai dari virus, pemerasan digital (*ransomware*), sampai serangan pemadaman layanan terdistribusi (DDoS) [3].

Agar pertahanan makin kuat, pengerasan sistem operasi (*hardening*) wajib dilakukan. Hardening adalah langkah antisipasi untuk meningkatkan ketangguhan sistem. Riset membuktikan bahwa jika pengerasan diterapkan dengan benar pada sistem operasi seperti Windows dan Linux, ketahanan sistem terhadap kemungkinan eksploitasi dan serangan digital bisa meningkat drastis [4].

Pengelolaan Pengguna di Sistem Operasi

Pengelolaan pengguna di sistem operasi berpusat pada penerapan aturan hak akses, termasuk prinsip hak akses sekecil mungkin (*least privilege*). Aturan ini menjamin tiap pengguna hanya punya wewenang yang benar-benar dibutuhkan. Kebijakan pengelolaan pengguna di sistem operasi harus didukung pengamanan di sisi jaringan.

Firewall dan pengaturan penyaringan situs web punya peran besar dalam menegakkan aturan keamanan. Dengan membatasi atau menyaring akses ke situs tertentu, firewall membantu pengelola mengontrol apa yang boleh dan tidak boleh dilakukan pengguna di jaringan, yang secara tidak langsung mendukung aturan pengelolaan pengguna dan menurunkan risiko keamanan [5].

Firewall

Firewall didefinisikan sebagai sistem pengaman yang mengatur aliran data antara jaringan dalam dan luar. Tugas utamanya adalah memantau, menyaring, dan mengontrol alur data, tujuannya melindungi jaringan dari ancaman dari luar serta menghalangi akses yang tidak sah [5].

Seberapa Ampuh Teknologi Firewall

Seberapa efektif firewall mencegah akses ilegal sangat tergantung pada teknologi dan pengaturannya. Dalam menghadapi ancaman masa kini, M. L. Yusuf dan rekan (2020) menunjukkan bahwa Firewall Generasi Terbaru (NGFW), dengan fitur Pencegahan Intrusi (IPS), jauh lebih baik dalam mendeteksi dan menghentikan serangan dibanding firewall lama [3]. Selain itu, kemanjuran ini sangat terikat pada pengaturan yang pas, misalnya penggunaan filter rules yang terbukti efektif mengurangi potensi serangan [6]. Efektivitas tertinggi baru tercapai jika firewall disesuaikan dan diatur dengan baik demi menjaga data penting [7].

Penelitian Terkait

Studi tentang seberapa efektif aturan keamanan menunjukkan beberapa kesimpulan penting. M. L. Yusuf dan rekan (2020) menguji kinerja Firewall Generasi Terbaru (NGFW) dan membuktikan keunggulannya dalam menangkal ancaman [3]. Sementara itu, Al Godzali dan rekan (2025) menilai kemanjuran pengerasan sistem operasi, membuktikan bahwa aturan keamanan yang menyeluruh di OS sangat krusial untuk ketangguhan sistem terhadap ancaman digital [4].

Dari sudut pandang penerapan dan kebijakan pengguna, D. A. Jakaria (2020) meneliti penerapan firewall dan penyaringan web di Mikrotik RouterOS, memperlihatkan bagaimana firewall bisa dipakai mendukung aturan internet sehat dan mencegah akses ke laman berbahaya [5]. Khusus tentang penataan, Reyfaldi dan Rahmatulloh (2024) meneliti penyesuaian konfigurasi firewall Mikrotik memakai metode filter rules dan membuktikan keampuhannya menghadapi serangan seperti brute force, yang sangat berhubungan dengan pencegahan akses ilegal [6]. Studi kasus oleh M. B. Yel dan rekan (2023) menggarisbawahi pentingnya penyesuaian konfigurasi firewall di infrastruktur jaringan untuk menjaga data penting tetap aman [7].

METODE PENELITIAN

Penelitian ini berupaya guna menganalisis efektivitas dari sebuah kebijakan manajemen user serta firewall pada sistem operasi untuk mencegah akses yang ilegal. Metode yang digunakan adalah metode kualitatif beserta dengan pendekatan studi literatur, yang sesuai sebab fokusnya yaitu pada pemahaman mendalam terhadap konsep teoritis beserta praktik kebijakan keamanan, bukan pengukuran angka ataupun eksperimen langsung[8]. Pendekatan ini memungkinkan penggalian penerapan teori keamanan dalam praktik, sesuai literatur yang ada, tanpa mengumpulkan data baru dari responden atau eksperimen lapangan. Cara ini pun efektif untuk topik ini, terkait keamanan sistem operasi sering terdokumentasi luas dalam jurnal juga panduan resmi.

Analisis data dijalankan dengan memakai teknik komparasi, saat dilakukan perbandingan konsep teoretis terhadap praktik implementasi pada sistem operasi Windows dan Linux. Proses ini dilakukan secara sistematis melalui pengumpulan data. Kemudian, dilakukan suatu Sintesis Konsep Teoritis serta perbandingan dengan Praktik Implementasi

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

yang ada. Guna menilai efektivitas kebijakan manajemen user beserta firewall, digunakan tiga metrik utama terukur berdasarkan literatur beserta studi kasus yaitu tingkat pencegahan akses ilegal, kemudahan Implementasi serta potensi kerentanan[9].

HASIL DAN PEMBAHASAN

Hasil Penelitian

Berdasarkan hasil kajian literatur terhadap berbagai penelitian nasional, diperoleh temuan bahwa kebijakan manajemen user dan firewall memiliki peran yang signifikan dalam mencegah akses ilegal pada sistem operasi. Manajemen user berfungsi sebagai mekanisme pengendalian hak akses internal, sementara firewall berperan sebagai pengaman lalu lintas jaringan dari ancaman eksternal. Kedua mekanisme ini saling melengkapi dalam membentuk sistem keamanan yang berlapis[10], [11].

Penerapan manajemen user yang baik ditandai dengan adanya pembatasan hak akses berdasarkan peran dan tanggung jawab pengguna. Pemisahan antara hak administrator dan pengguna biasa mampu mengurangi risiko penyalahgunaan sistem oleh pihak internal[10], [12]. Dengan adanya pembatasan tersebut, akses terhadap sumber daya sistem menjadi lebih terkontrol dan sesuai dengan kebutuhan operasional pengguna.

Pada sisi jaringan, firewall terbukti efektif dalam membatasi akses ilegal dari luar sistem. Firewall yang dikonfigurasi dengan aturan yang tepat mampu menyaring lalu lintas jaringan, menutup port yang tidak diperlukan, serta meminimalkan potensi serangan dari jaringan eksternal[11]. Hasil kajian menunjukkan bahwa firewall dapat menjadi garis pertahanan awal dalam melindungi sistem operasi dari ancaman berbasis jaringan.

Selain itu, perbandingan implementasi pada sistem operasi Windows dan Linux menunjukkan adanya perbedaan dalam pendekatan keamanan. Windows cenderung menawarkan kemudahan pengelolaan keamanan melalui sistem terpusat, sedangkan Linux memberikan fleksibilitas yang lebih tinggi dalam pengaturan hak akses secara granular[13]. Meskipun demikian, keduanya sama-sama menyediakan mekanisme keamanan yang efektif apabila dikonfigurasi dengan benar.

Pembahasan

Hasil penelitian menunjukkan bahwa efektivitas kebijakan manajemen user sangat bergantung pada konsistensi penerapan prinsip pembatasan hak akses. Dengan membatasi hak pengguna hanya pada fungsi yang diperlukan, potensi akses ilegal maupun eskalasi hak akses dapat ditekan[12]. Hal ini membuktikan bahwa manajemen user merupakan komponen fundamental dalam keamanan sistem operasi, terutama dalam mencegah dari pengguna internal.

Firewall berfungsi sebagai lapisan perlindungan tambahan yang melengkapi kebijakan manajemen user[11]. Dengan mengontrol lalu lintas data yang masuk dan keluar dari sistem, firewall mampu mencegah akses ilegal sebelum mencapai lapisan sistem operasi. Namun, efektivitas firewall sangat dipengaruhi oleh ketepatan konfigurasi dan pembaruan aturan keamanan secara berkala.

Dari sisi kemudahan implementasi, terdapat perbedaan tingkat kompleksitas antara sistem operasi. Sistem yang menyediakan antarmuka pengelolaan terpusat cenderung lebih mudah diterapkan, tetapi sistem dengan fleksibilitas konfigurasi tinggi memerlukan pemahaman teknis yang lebih mendalam[13]. Oleh karena itu, kompetensi administrator sistem menjadi faktor penting dalam menentukan keberhasilan penerapan kebijakan keamanan.

Meskipun mekanisme keamanan telah tersedia, potensi kerentanan tetap dapat muncul akibat kesalahan konfigurasi dan kurangnya evaluasi berkala. Hal ini menunjukkan bahwa kebijakan keamanan sistem operasi tidak hanya bergantung pada teknologi, tetapi juga pada faktor manusia dan prosedur pengelolaan yang diterapkan. Dengan demikian, kombinasi antara kebijakan yang tepat, konfigurasi yang benar, dan pengawasan berkelanjutan menjadi kunci dalam meningkatkan efektivitas pencegahan akses ilegal.

KESIMPULAN

Berdasarkan hasil kajian dan penelitian, dapat disimpulkan bahwa kebijakan manajemen user dan firewall memiliki peranan yang cukup signifikan dalam mencegah akses ilegal pada sistem operasi. Keduanya saling melengkapi dalam membentuk sistem keamanan yang berlapis. Manajemen user berfungsi sebagai pengendali hak akses internal dengan adanya pembatasan hak pengguna sesuai peran dan tanggung jawabnya, sehingga dapat mengurangi risiko penyalahgunaan hak akses dari dalam sistem serta mengontrol akses terhadap sumber daya sistem.

Firewall berperan sebagai lapisan pertahanan eksternal yang efektif dalam mengendalikan lalu lintas jaringan dan mencegah akses ilegal dari luar sistem. Firewall yang dikonfigurasi dengan tepat mampu menyaring lalu lintas jaringan, menutup port yang tidak diperlukan, serta menekan potensi terjadinya serangan berbasis jaringan sebelum mencapai sistem operasi.

Hasil pembahasan juga menunjukkan bahwa efektivitas kedua kebijakan tersebut sangat bergantung pada konsistensi penerapan, ketepatan konfigurasi, serta kompetensi administrator sistem. Perbandingan implementasi pada sistem operasi Windows dan Linux memperlihatkan bahwa meskipun memiliki pendekatan yang berbeda, keduanya

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

sama-sama dapat memberikan tingkat keamanan yang optimal apabila kebijakan manajemen user dan firewall diterapkan secara tepat dan berkelanjutan.

Secara keseluruhan temuan ini menunjukkan bahwa kebijakan keamanan sistem operasi tidak hanya bergantung pada teknologi, tetapi juga pada faktor manusia dan prosedur pengelolaan yang diterapkan. Dengan demikian, kombinasi antara manajemen user yang baik dan firewall yang efektif dapat membentuk sistem keamanan berlapis yang mampu meningkatkan perlindungan terhadap akses ilegal pada sistem operasi.

REFERENSI

[1] NIST SP800-53, "Security and Privacy Controls for Information Systems and Organizations," *NIST Spec. Publ.*, p. 465, 2020, [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5

[2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "NIST Special Publication 800-207," 2022.

[3] M. Lutfi Yusuf, K. Karsono, N. Budhisantosa, J. Arjuna No, and K. Jeruk Jakarta Barat DKI Jakarta, "Analisis Performance Next Generation Firewall Dan Mikrotik Rb1100 Sebagai Firewall Untuk Keamanan Jaringan JIK," *J. Ilmu Komput.*, vol. 5, no. 1, pp. 15–30, 2020.

[4] A. R. Kannajmi *et al.*, "Evaluasi Efektivitas Hardening dalam Meningkatkan Keamanan Sistem Operasi Windows dan Linux," *IJINF (Internal J. Informatics) Eval.*, pp. 1–17, 2025.

[5] A. Ramadhani, N. Palasara, and A. Gani, "Filtering Firewall dan Manajemen Bandwidth untuk Keamanan Jaringan pada Kelurahan Buaran Indah," *Remik*, vol. 9, no. 1, pp. 346–355, 2025, doi: 10.33395/remik.v9i1.14482.

[6] A. N. Reyfaldi and A. Rahmatulloh, "Optimalisasi Konfigurasi Firewall MikroTik Menggunakan Metode Filter Rules Untuk Keamanan Jaringan," *J. Inform. dan Ris.*, vol. 2, no. 2, pp. 5–12, 2024, [Online]. Available: https://ejournal.bhamada.ac.id/index.php/IRIS/article/view/744%0Ahttps://ejournal.bhamada.ac.id/index.php/IRIS

[7] M. B. Yel, D. I. Mulyana, J. R. F, M. D. Nurfaishal, and M. H. T. B, "Optimalisasi Keamanan Firewall Pada Infrastruktur Jaringan Smk Idn Bogor," *J. Cahaya Mandalika*, vol. 4, no. 1, pp. 594–610, 2023, [Online]. Available: https://www.ojs.cahayamandalika.com/index.php/JCM/article/view/1393

[8] R. Al Fajar, A. Lestari, and J. Teknologi Informasi, "Analisis Perbandingan Sistem Operasi Windows 11 dan Linux Ubuntu Menggunakan Metode Studi Literatur (Studi Kasus: Kinerja Sistem, Keamanan dan Biaya)," *J. Bitwise ISSN xxxx-xxxx*, vol. 1, no. 2, pp. 74–82, 2025, [Online]. Available: https://jurnal-bitwise.org/

[9] H. P. Fitrian, B. F. Noorjamil, F. Rahmawati, and S. A. Rachman, "Analisis Efektivitas Firewall dalam Memfilter dan Melindungi Lalu Lintas Jaringan," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 8, no. 1, pp. 95–102, 2025, doi: 10.32672/jnkti.v8i1.8554.

[10] C. A. Gemawaty and Y. Yuliani, "Manajemen Identitas Dan Akses Dalam Keamanan Sistem Informasi (Pendekatan Literature Review)," *J. Manaj. Inform. Jayakarta*, vol. 4, no. 4, pp. 396–403, 2024, [Online]. Available: http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

[11] B. R. Lesmana, A. Junaidi, and A. N. Sihananto, "Analisis Pengujian Keamanan Firewall Pada Sistem X Di Universitas Z," *J. Inf. Syst. Applied, Manag. Account. Res.*, vol. 8, no. 3, p. 557, 2024, doi: 10.52362/jisamar.v8i3.1563.

[12] Y. Yuricha and I. K. Phan, "Penerapan Role Based Access Control dalam Sistem Supply Chain Management Berbasis Cloud," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 3, no. 2, pp. 339–348, 2023, doi: 10.57152/malcom.v3i2.1259.

[13] G. Al Godzali, R. I. Athallah, and E. Rivalni, "Evaluasi Keamanan Autentikasi Pengguna pada Sistem Operasi Windows dan Linux," *Neptunus J. Ilmu Komput. dan Tekknologi Inf.*, vol. 3, no. 1, pp. 31–40, 2025.