

Optimalisasi penggunaan firewall dalam meningkatkan keamanan pada sistem operasi

Syamsul Bahri

Universitas Pertiwi, Bekasi, Jawa Barat, Indonesia

Corresponding Author e-mail: syamsul.bahri@pertiwi.ac.id

Abstrak

Sistem operasi Windows 11 merupakan salah satu sistem operasi yang banyak digunakan oleh pengguna komputer sehingga memiliki risiko menjadi sasaran berbagai ancaman siber, seperti malware, spyware, ransomware, trojan, pencurian data, dan kerusakan sistem. Kondisi tersebut menunjukkan pentingnya penerapan langkah preventif untuk meningkatkan keamanan sistem. Salah satu fitur keamanan yang telah tersedia pada Windows 11 adalah firewall. Namun, keberadaan firewall belum sepenuhnya dimanfaatkan secara optimal oleh pengguna karena masih terdapat keterbatasan pengetahuan dan pemahaman mengenai konfigurasi serta fungsi keamanan sistem. Penelitian ini bertujuan untuk menganalisis optimalisasi penggunaan firewall dalam sistem operasi Windows 11 sebagai upaya preventif untuk meningkatkan keamanan dan perlindungan sistem dari berbagai ancaman siber. Penelitian menggunakan metode deskriptif kualitatif dengan pendekatan studi literatur dan observasi sistem. Data diperoleh melalui observasi konfigurasi keamanan Windows 11, studi terhadap buku, jurnal, prosiding, dan dokumentasi teknis, serta dokumentasi berupa panduan dan tangkapan layar konfigurasi sistem. Analisis data dilakukan melalui tahap reduksi data, penyajian data, dan penarikan kesimpulan. Hasil penelitian menunjukkan bahwa firewall Windows 11 memiliki fungsi penting dalam mengawasi, mengontrol, dan menyaring lalu lintas data yang masuk dan keluar dari sistem. Optimalisasi firewall dapat diterapkan pada jaringan domain, jaringan pribadi, dan jaringan publik sesuai dengan karakteristik serta tingkat risikonya. Kesimpulannya, optimalisasi penggunaan firewall bawaan Windows 11 merupakan salah satu langkah preventif yang dapat membantu meningkatkan keamanan sistem dan mengurangi risiko serangan siber serta kehilangan data.

Kata kunci : *Windows 11, Sistem Operasi, Firewall, Preventif Keamanan*

Abstract

Windows 11 is a widely used operating system, making it a frequent target for various cyber threats such as malware, spyware, ransomware, Trojans, data theft, and system damage. This situation highlights the importance of implementing preventive measures to enhance system security. One of the security features available in Windows 11 is the firewall; however, users often fail to fully utilize it due to limited knowledge and understanding regarding its configuration and security functions. This study aims to analyze the optimization of firewall usage in Windows 11 as a preventive measure to improve system security and protection against various cyber threats. The research employs a qualitative descriptive method, utilizing a literature review and system observation. Data were gathered through observations of Windows 11 security configurations; reviews of books, journals, proceedings, and technical documentation; and the collection of system configuration guides and screenshots. Data analysis involved data reduction, data presentation, and conclusion drawing. The results indicate that the Windows 11 firewall plays a crucial role in monitoring, controlling, and filtering data traffic entering and leaving the system. Firewall optimization can be implemented across domain, private, and public networks, tailored to their specific characteristics and risk levels. In conclusion, optimizing the built-in Windows 11 firewall serves as a preventive measure that helps enhance system security while reducing the risk of cyberattacks and data loss.

Keywords: *Windows 11, operating system, firewall, preventive security*

How to Cite: Syamsul Bahri. (2026). Optimalisasi penggunaan firewall dalam meningkatkan keamanan pada sistem operasi. *Journal Transformation of Mandalika*, E-ISSN: 2745-5882, P-ISSN: 2962-2956 , 7(8), 1044-1053.



<https://doi.org/10.36312/jtm.v7i8.6745>

Copyright©2026, Author (s)

This is an open-access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) License.



PENDAHULUAN

Perkembangan teknologi informasi telah menjadikan sistem operasi sebagai komponen penting dalam mendukung berbagai aktivitas komputasi, baik untuk keperluan pribadi, pendidikan, bisnis, maupun organisasi. Sistem operasi berfungsi sebagai perangkat lunak utama yang mengatur sumber daya perangkat keras, menjalankan aplikasi, mengelola memori, penyimpanan, proses, serta menyediakan mekanisme keamanan bagi pengguna. Salah satu sistem operasi yang banyak digunakan saat ini adalah Windows 11 yang dikembangkan sebagai penerus Windows 10. Windows 11 menawarkan sejumlah peningkatan dibandingkan versi sebelumnya, terutama dari aspek keandalan, kompatibilitas, dan keamanan sistem. Meskipun demikian, peningkatan fitur keamanan tidak secara otomatis menghilangkan risiko terhadap ancaman siber karena keamanan suatu sistem juga sangat dipengaruhi oleh bagaimana pengguna memanfaatkan dan mengonfigurasi fitur keamanan yang tersedia. Dalam konteks ini, pemanfaatan mekanisme keamanan secara tepat menjadi bagian penting dalam menjaga keberlangsungan dan perlindungan sistem komputer (Usman et al., 2019; Pratama, 2018).. (Usman et al., 2019; Pratama, 2018; Dwinanto & Setiyani, 2021).

Windows 11 diperkenalkan pada tahun 2021 dengan berbagai pembaruan yang diarahkan untuk meningkatkan pengalaman dan keamanan pengguna. Perkembangan tersebut menunjukkan adanya perhatian terhadap aspek keamanan sistem operasi, terutama karena lingkungan komputasi modern menghadapi ancaman yang semakin beragam. Namun, keberadaan fitur keamanan pada sistem operasi tidak berarti bahwa sistem akan sepenuhnya terbebas dari serangan. Sistem komputer tetap dapat menjadi sasaran malware, phishing, ransomware, trojan, pencurian data, maupun eksploitasi terhadap celah keamanan. Ancaman tersebut dapat menyebabkan gangguan terhadap kinerja sistem, kehilangan data, kerusakan perangkat lunak, hingga akses tidak sah terhadap informasi pengguna. Chowdhury et al. (2020) menjelaskan bahwa keamanan komputer berkaitan dengan berbagai upaya untuk melindungi sistem dan informasi dari tindakan yang dapat mengganggu kerahasiaan, integritas, maupun ketersediaan data. Oleh karena itu, peningkatan fitur keamanan harus diikuti dengan penerapan mekanisme perlindungan yang tepat pada tingkat pengguna maupun sistem. (Ramdhani et al., 2026; Supriyanto et al., 2026).

Fenomena keamanan tersebut menjadi semakin penting karena sebagian risiko keamanan bukan hanya berasal dari kelemahan teknologi, tetapi juga dari kelalaian pengguna dalam menerapkan fungsi keamanan dasar. Dalam praktik penggunaan Windows 11, pengguna dapat mengabaikan pembaruan sistem, menggunakan kata sandi yang lemah, tidak memperhatikan jenis jaringan yang digunakan, atau tidak melakukan konfigurasi firewall secara optimal. Kondisi tersebut dapat meningkatkan peluang terjadinya akses yang tidak diinginkan terhadap sistem. Penelitian Hidayat dan Prasetyo (2021) yang tercantum dalam referensi artikel menempatkan keamanan sistem informasi dalam konteks pengelolaan risiko teknologi informasi, sedangkan Kurniawan dan Nugroho (2020) membahas penerapan keamanan jaringan dengan pendekatan berlapis. Kedua kajian tersebut menunjukkan pentingnya penerapan mekanisme keamanan yang tidak hanya bergantung pada satu komponen, tetapi dilakukan melalui penguatan berbagai aspek perlindungan sistem. Dalam penelitian ini, salah satu aspek yang menjadi perhatian adalah optimalisasi firewall sebagai mekanisme preventif pada sistem operasi Windows 11. (Chowdhury et al., 2020; Hidayat & Prasetyo, 2021).

Firewall merupakan salah satu komponen penting dalam keamanan komputer dan jaringan karena berfungsi untuk mengawasi serta mengendalikan lalu lintas data yang masuk maupun keluar dari sistem. Secara konseptual, firewall dapat digunakan untuk memisahkan lalu lintas yang dipercaya dan tidak dipercaya serta membantu mengendalikan akses berdasarkan aturan keamanan yang telah ditentukan (Khoumsi et al., 2018; Hu et al., 2019). Firewall dapat berbentuk perangkat keras maupun perangkat lunak. Pada Windows 11, fungsi firewall telah tersedia sebagai bagian dari sistem keamanan bawaan sehingga pengguna tidak selalu membutuhkan perangkat tambahan untuk memperoleh perlindungan dasar terhadap lalu lintas jaringan. Keberadaan firewall bawaan tersebut memberikan peluang bagi pengguna untuk menerapkan tindakan preventif secara langsung melalui sistem operasi. Namun, keberadaan fitur tersebut perlu diikuti dengan pemahaman mengenai fungsi, konfigurasi, dan penerapannya sesuai dengan kondisi jaringan yang digunakan. (Khoumsi et al., 2018; Hu et al., 2019; Li et al., 2019).

Penerapan firewall menjadi semakin relevan ketika komputer terhubung dengan berbagai jenis jaringan. Windows 11 menyediakan pengaturan firewall yang dapat diterapkan pada jaringan domain, jaringan pribadi, dan jaringan publik. Jaringan domain umumnya berkaitan dengan lingkungan organisasi atau perusahaan yang memiliki kebijakan keamanan tertentu. Jaringan pribadi lebih banyak digunakan pada lingkungan rumah atau jaringan yang relatif terbatas, sedangkan jaringan publik memiliki tingkat risiko yang lebih tinggi karena dapat digunakan oleh banyak pihak dan tidak selalu berada dalam lingkungan yang dapat dikendalikan oleh pengguna. Perbedaan karakteristik jaringan tersebut menunjukkan bahwa konfigurasi keamanan tidak dapat dilakukan secara sembarangan. Pengguna perlu memahami kondisi jaringan yang sedang digunakan dan memastikan bahwa firewall berfungsi sesuai dengan kebutuhan perlindungan sistem. Optimalisasi firewall dengan mempertimbangkan karakteristik jaringan menjadi salah satu langkah preventif

yang dapat dilakukan untuk mengurangi potensi ancaman terhadap komputer Windows 11. (Alicea & Alsmadi, 2021; Kim et al., 2021; Lee et al., 2021).

Penelitian terdahulu mengenai keamanan komputer dan jaringan telah memberikan perhatian terhadap penggunaan firewall sebagai salah satu mekanisme perlindungan. Wicaksono (2022), sebagaimana tercantum dalam daftar referensi penelitian, membahas sistem keamanan jaringan dengan menggunakan firewall melalui metode port blocking dan firewall filtering. Kajian tersebut menunjukkan bahwa firewall dapat dimanfaatkan untuk mengendalikan lalu lintas jaringan berdasarkan aturan tertentu. Sementara itu, Kurniawan dan Nugroho (2020) membahas implementasi keamanan jaringan komputer menggunakan pendekatan layered security, yang menekankan pentingnya penerapan keamanan melalui beberapa lapisan perlindungan. Dwinanto dan Setiyani (2021) juga membahas implementasi keamanan komputer pada aspek confidentiality, integrity, dan availability dengan menggunakan tools audit sistem. Berbagai penelitian tersebut memperlihatkan bahwa keamanan komputer membutuhkan mekanisme perlindungan yang sistematis dan dapat disesuaikan dengan karakteristik ancaman yang dihadapi. (Wicaksono, 2022; Kurniawan & Nugroho, 2020; Hadi et al., 2026).

Selain kajian mengenai firewall dan keamanan jaringan, penelitian mengenai keamanan sistem operasi juga telah dilakukan untuk mengidentifikasi berbagai ancaman dalam lingkungan teknologi informasi modern. Pratama (2018) membahas ancaman keamanan sistem operasi pada lingkungan teknologi informasi modern, sedangkan Hidayat dan Prasetyo (2021) mengkaji keamanan sistem informasi berbasis manajemen risiko teknologi informasi. Kajian tersebut memberikan dasar bahwa ancaman terhadap sistem komputer perlu dipahami melalui pendekatan pencegahan dan pengelolaan risiko. Usman et al. (2019) juga menempatkan keamanan komputer sebagai bidang yang mencakup perlindungan sistem dari berbagai bentuk ancaman dan serangan. Dengan demikian, penggunaan firewall tidak seharusnya dipandang hanya sebagai fitur tambahan, tetapi sebagai salah satu bagian dari mekanisme keamanan sistem yang perlu dipahami dan dimanfaatkan secara tepat oleh pengguna. (Pratama, 2018; Beaman et al., 2021).

Meskipun penelitian mengenai keamanan jaringan, firewall, dan keamanan komputer telah cukup banyak dilakukan, masih terdapat kesenjangan dalam kajian yang secara khusus membahas optimalisasi fungsi firewall bawaan pada sistem operasi Windows 11 sebagai pendekatan preventif. Penelitian Wicaksono (2022) lebih menekankan penggunaan firewall untuk port blocking dan firewall filtering, sedangkan kajian Kurniawan dan Nugroho (2020) berorientasi pada pendekatan keamanan berlapis. Sementara itu, penelitian terkait keamanan sistem operasi lebih banyak membahas ancaman dan aspek keamanan secara umum. Berdasarkan telaah terhadap penelitian yang dicantumkan dalam artikel, kajian yang secara spesifik menghubungkan penggunaan firewall bawaan Windows 11 dengan upaya preventif untuk meningkatkan perlindungan sistem masih perlu diperkuat. Research gap tersebut menjadi dasar penting bagi penelitian ini untuk memberikan pembahasan yang lebih terarah mengenai pemanfaatan firewall yang telah tersedia pada Windows 11. (Buck et al., 2021; Ferretti et al., 2021; Sengupta & Lakshminarayanan, 2021).

Kesenjangan penelitian tersebut sekaligus menunjukkan urgensi penelitian. Pengguna Windows 11 tidak hanya membutuhkan informasi mengenai keberadaan firewall, tetapi juga membutuhkan pemahaman mengenai bagaimana fungsi tersebut dapat digunakan secara optimal sesuai dengan kondisi sistem dan jaringan. Firewall yang tersedia tetapi tidak dikonfigurasi atau dimanfaatkan secara tepat dapat mengurangi efektivitas perlindungan yang seharusnya diberikan. Oleh sebab itu, pendekatan preventif perlu dikembangkan dengan menempatkan firewall sebagai salah satu mekanisme awal untuk mengendalikan lalu lintas data dan mengurangi peluang terjadinya akses yang tidak diinginkan. Pendekatan preventif lebih menekankan tindakan sebelum serangan terjadi daripada hanya melakukan penanganan setelah sistem mengalami gangguan. Dalam konteks keamanan komputer, tindakan pencegahan menjadi penting karena kerusakan sistem dan kehilangan data dapat menimbulkan dampak yang lebih besar dibandingkan upaya perlindungan yang dilakukan sejak awal (Chowdhury et al., 2020). (Mosteiro-Sanchez et al., 2020; Alexander, 2020).

Optimalisasi firewall juga memiliki urgensi praktis karena Windows 11 telah menyediakan fungsi firewall sebagai bagian dari sistem operasinya. Dengan demikian, pengguna dapat memanfaatkan fasilitas keamanan yang tersedia tanpa harus selalu bergantung pada perangkat keamanan eksternal. Firewall dapat membantu mengawasi, mengontrol, dan menyaring lalu lintas data yang masuk dan keluar dari sistem. Penggunaan firewall secara tepat pada jaringan domain, pribadi, dan publik dapat menjadi bagian dari strategi perlindungan yang disesuaikan dengan tingkat risiko masing-masing jaringan. Dalam lingkungan publik, misalnya, pengguna perlu memberikan perhatian lebih besar terhadap potensi akses dari pihak yang tidak dikenal. Sebaliknya, pada jaringan pribadi maupun domain, pengaturan firewall perlu disesuaikan dengan kebijakan dan kebutuhan lingkungan jaringan. Hal tersebut menunjukkan bahwa optimalisasi firewall tidak hanya berkaitan dengan mengaktifkan fitur, tetapi juga memahami fungsi dan penerapannya sesuai dengan kondisi penggunaan. (McIntosh et al., 2021; Beaman et al., 2021).

Berdasarkan uraian tersebut, penelitian mengenai optimalisasi penggunaan firewall dalam sistem operasi Windows 11 penting dilakukan untuk memberikan pemahaman mengenai pemanfaatan fitur keamanan bawaan sebagai salah satu upaya preventif. Penelitian ini menggunakan pendekatan deskriptif kualitatif melalui

studi literatur dan observasi sistem untuk memahami serta menganalisis penerapan keamanan firewall pada Windows 11. Observasi dilakukan terhadap konfigurasi keamanan Windows 11, sedangkan studi literatur digunakan untuk mengkaji buku, jurnal, prosiding, dan dokumentasi teknis yang berkaitan dengan keamanan sistem operasi dan firewall. Data selanjutnya dianalisis melalui reduksi data, penyajian data, dan penarikan kesimpulan sehingga diperoleh gambaran mengenai penerapan firewall sebagai mekanisme perlindungan sistem. (Khoumsi et al., 2018; Kim et al., 2021; Alicea & Alsmadi, 2021).

Berdasarkan latar belakang, fenomena, hasil penelitian terdahulu, research gap, dan urgensi tersebut, penelitian ini diarahkan untuk menjawab pertanyaan utama: bagaimana optimalisasi penggunaan firewall bawaan pada sistem operasi Windows 11 dapat diterapkan sebagai upaya preventif untuk meningkatkan keamanan sistem dan mengurangi risiko serangan siber? Secara khusus, penelitian ini bertujuan untuk menganalisis penerapan optimalisasi fungsi firewall pada Windows 11, mengidentifikasi pemanfaatannya pada berbagai jenis jaringan, serta menjelaskan perannya sebagai mekanisme preventif dalam perlindungan sistem. Hasil penelitian diharapkan dapat memberikan kontribusi praktis bagi pengguna Windows 11 dalam memahami dan memanfaatkan fungsi firewall secara lebih optimal serta memberikan kontribusi akademik sebagai referensi dalam kajian keamanan sistem operasi dan perlindungan data. (Buck et al., 2021; Ferretti et al., 2021; McIntosh et al., 2021).

METODE PENELITIAN

Jenis dan Desain Penelitian

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi literatur dan observasi sistem. Pemilihan pendekatan ini didasarkan pada tujuan penelitian, yaitu memahami dan menganalisis penerapan pendekatan preventif dalam optimalisasi keamanan sistem operasi Windows 11, khususnya melalui pemanfaatan fungsi firewall bawaan. Pendekatan deskriptif kualitatif digunakan untuk menggambarkan fenomena keamanan sistem secara sistematis berdasarkan data yang diperoleh melalui pengamatan sistem dan penelaahan berbagai sumber literatur. Dalam konteks keamanan komputer, sistem operasi memiliki fungsi penting dalam mengelola proses, memori, penyimpanan, serta aspek keamanan sistem sehingga mekanisme perlindungan perlu dianalisis secara menyeluruh (Usman et al., 2019; Pratama, 2018).. (Hidayat & Prasetyo, 2021; Dwinanto & Setiyani, 2021).

Desain penelitian diarahkan pada analisis konseptual dan praktis terhadap fungsi firewall sebagai mekanisme preventif. Analisis konseptual dilakukan melalui kajian literatur yang berkaitan dengan keamanan komputer, keamanan sistem operasi, dan firewall, sedangkan analisis praktis dilakukan melalui observasi terhadap konfigurasi dan fungsi firewall pada Windows 11. Firewall dipahami sebagai mekanisme yang berfungsi mengawasi dan menyaring lalu lintas data yang masuk dan keluar dari sistem (Khoumsi et al., 2018; Hu et al., 2019). (Khoumsi et al., 2018; Hu et al., 2019; Kim et al., 2021).

Lokasi dan Waktu Penelitian

Penelitian ini tidak dilakukan pada lokasi lapangan tertentu karena menggunakan studi literatur dan observasi terhadap sistem operasi Windows 11. Oleh karena itu, lokasi penelitian berupa lingkungan sistem komputer yang menggunakan Windows 11 sebagai objek observasi. Waktu pelaksanaan penelitian tidak dicantumkan secara spesifik dalam naskah awal, sehingga informasi waktu penelitian perlu disesuaikan dengan waktu pelaksanaan sebenarnya oleh peneliti.

Objek Penelitian

Objek penelitian adalah mekanisme preventif keamanan pada sistem operasi Windows 11, khususnya fungsi firewall bawaan. Pemilihan firewall sebagai objek didasarkan pada perannya dalam mengawasi, mengontrol, dan menyaring lalu lintas data yang masuk dan keluar dari sistem. Analisis juga memperhatikan penerapan firewall pada jaringan domain, jaringan pribadi, dan jaringan publik karena masing-masing memiliki karakteristik dan tingkat risiko yang berbeda. (Alicea & Alsmadi, 2021; Lee et al., 2021).

Penelitian ini tidak menggunakan populasi dan sampel dalam pengertian penelitian kuantitatif. Subjek penelitian berupa sistem atau konfigurasi firewall Windows 11 yang diamati untuk memperoleh informasi mengenai penerapan mekanisme keamanan preventif.

Teknik Pengumpulan Data

Data penelitian dikumpulkan melalui tiga teknik, yaitu observasi sistem, studi literatur, dan dokumentasi.

Pertama, observasi sistem dilakukan dengan mengamati konfigurasi keamanan pada sistem operasi Windows 11 untuk mengidentifikasi keberadaan, fungsi, dan penerapan Windows Firewall. Observasi difokuskan pada mekanisme firewall dalam mengontrol lalu lintas jaringan serta penerapannya pada jaringan domain, pribadi, dan publik. (Liu et al., 2020; Yu & Bian, 2020).

Kedua, studi literatur dilakukan dengan menelaah buku, jurnal, prosiding, dan dokumentasi teknis yang relevan dengan keamanan sistem operasi, keamanan komputer, dan firewall. Literatur mengenai keamanan komputer

digunakan sebagai landasan untuk memahami mekanisme perlindungan sistem, termasuk konsep firewall sebagai pemisah dan pengendali jaringan terpercaya dan tidak terpercaya (Khoumsi et al., 2018; Chowdhury et al., 2020). (Usman et al., 2019; Alexander, 2020).

Ketiga, dokumentasi dilakukan dengan mengumpulkan panduan teknis, tangkapan layar konfigurasi sistem, dan catatan implementasi keamanan yang mendukung proses analisis. Dokumentasi digunakan sebagai bukti pendukung hasil observasi terhadap konfigurasi firewall Windows 11.

Instrumen Penelitian

Instrumen penelitian berupa lembar observasi, pedoman studi literatur, dan format dokumentasi. Lembar observasi digunakan untuk mencatat konfigurasi dan fungsi firewall Windows 11, pedoman studi literatur digunakan untuk mengidentifikasi informasi yang relevan dari sumber pustaka, sedangkan format dokumentasi digunakan untuk mencatat dan mengorganisasikan tangkapan layar, panduan teknis, serta catatan hasil pengamatan.

Teknik Analisis Data

Data dianalisis menggunakan teknik deskriptif kualitatif melalui tiga tahapan, yaitu reduksi data, penyajian data, dan penarikan kesimpulan. Reduksi data dilakukan dengan menyeleksi dan menyederhanakan informasi yang relevan dengan optimalisasi firewall. Penyajian data dilakukan dengan mengorganisasikan hasil observasi, literatur, dan dokumentasi dalam bentuk uraian deskriptif yang sistematis. Selanjutnya, penarikan kesimpulan dilakukan melalui interpretasi hasil analisis untuk mengidentifikasi efektivitas penerapan firewall sebagai mekanisme preventif dalam meningkatkan keamanan sistem operasi Windows 11.

Kerangka Analisis

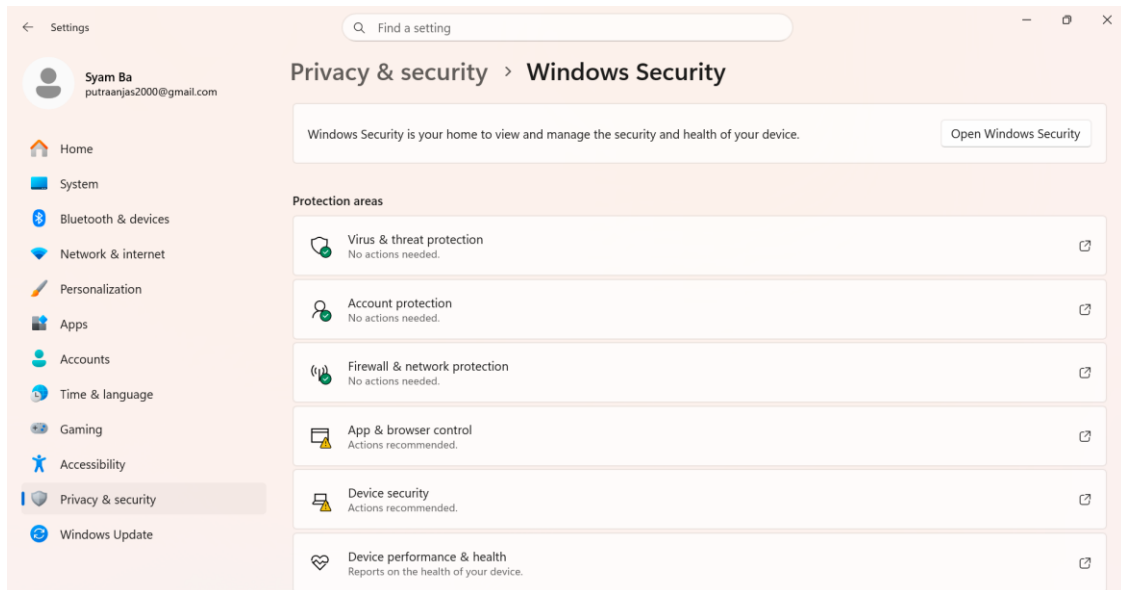
Kerangka analisis penelitian berfokus pada konsep pencegahan keamanan dengan menitikberatkan pada firewall standar bawaan Windows 11. Analisis dilakukan dengan menghubungkan fungsi firewall sebagai pengawas dan penyaring lalu lintas data dengan kebutuhan perlindungan sistem terhadap berbagai ancaman siber. Kerangka tersebut digunakan untuk menjelaskan bagaimana optimalisasi fungsi firewall dapat mendukung upaya preventif dalam meningkatkan keamanan sistem Windows 11. (Mosteiro-Sanchez et al., 2020; Buck et al., 2021).

PEMBAHASAN

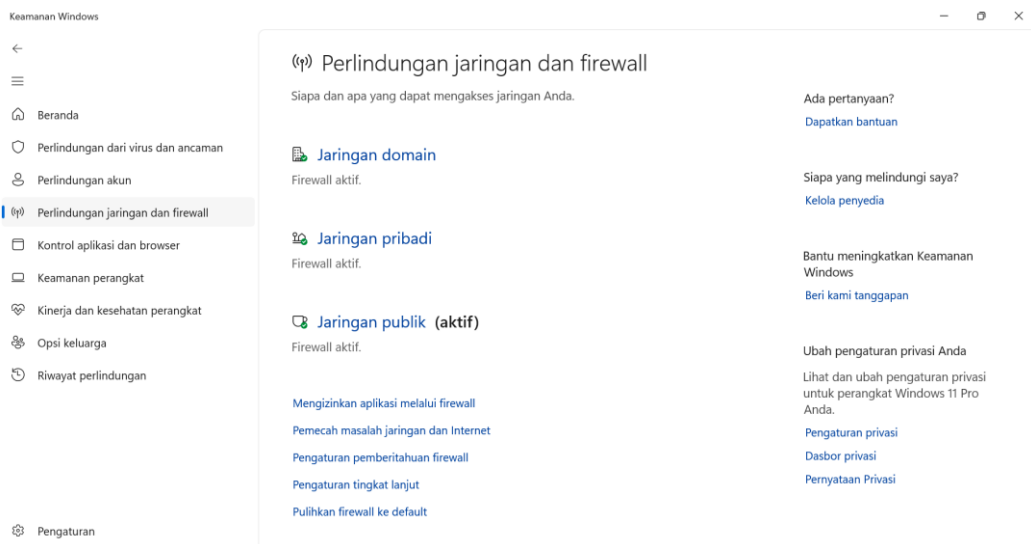
Firewall merupakan salah satu perangkat yang sangat penting untuk menjaga sistem. Berdasarkan bentuk fisiknya firewall itu berbentuk *hardware* yaitu perangkat berbentuk fisik yang dipasang antara jaringan internal dan internet, sedangkan yang *software*, berbentuk non fisik yang berbentuk aplikasi atau program yang bisa dipasang dalam sistem operasi seperti di windows 11, pihak Microsoft sudah langsung membuat firewall dalam windows 11. Fungsi firewall windows 11 adalah untuk mengawasi, mengontrol, dan menyaring data yang masuk dan keluar. (Hu et al., 2019; Li et al., 2019; Khoumsi et al., 2018).

Hasil penelitian menunjukkan bahwa firewall merupakan salah satu komponen penting dalam mekanisme keamanan sistem operasi Windows 11. Berdasarkan hasil observasi sistem dan studi literatur, firewall pada Windows 11 telah tersedia sebagai fitur keamanan bawaan yang dapat digunakan untuk mengawasi, mengontrol, dan menyaring lalu lintas data yang masuk maupun keluar dari sistem. Keberadaan firewall bawaan tersebut memberikan fasilitas perlindungan awal bagi pengguna tanpa harus selalu memasang perangkat lunak firewall tambahan. Temuan ini memperlihatkan bahwa Windows 11 telah menyediakan salah satu mekanisme preventif yang dapat dimanfaatkan untuk mengurangi risiko akses jaringan yang tidak diinginkan. Dalam perspektif keamanan komputer, mekanisme perlindungan terhadap sistem diperlukan untuk mencegah akses atau tindakan yang dapat mengganggu sistem dan informasi pengguna (Chowdhury et al., 2020). (Ramdhani et al., 2026; Supriyanto et al., 2026).

Secara konseptual, hasil penelitian juga menunjukkan bahwa firewall dapat dibedakan berdasarkan bentuk penerapannya menjadi firewall berbasis perangkat keras dan perangkat lunak. Firewall perangkat keras merupakan perangkat fisik yang ditempatkan di antara jaringan internal dan jaringan internet, sedangkan firewall perangkat lunak berbentuk aplikasi atau program yang terintegrasi dengan sistem operasi. Pada Windows 11, firewall perangkat lunak telah menjadi bagian dari sistem keamanan bawaan. Fungsi tersebut memungkinkan sistem untuk melakukan pengawasan terhadap lalu lintas jaringan serta mengendalikan komunikasi data yang masuk dan keluar. Temuan ini sesuai dengan konsep firewall yang dikemukakan Khoumsi et al. (2018), bahwa firewall berfungsi sebagai mekanisme yang memantau dan memisahkan jaringan atau lalu lintas yang dipercaya dan tidak dipercaya. Dengan demikian, firewall tidak hanya berfungsi sebagai fitur teknis, tetapi juga menjadi salah satu lapisan perlindungan dalam keamanan sistem komputer. (Kim et al., 2021; Lee et al., 2021; Alicea & Alsmadi, 2021).



Gambar 1 : Posisi Firewall



Gambar 2 ; Perlindungan Firewall

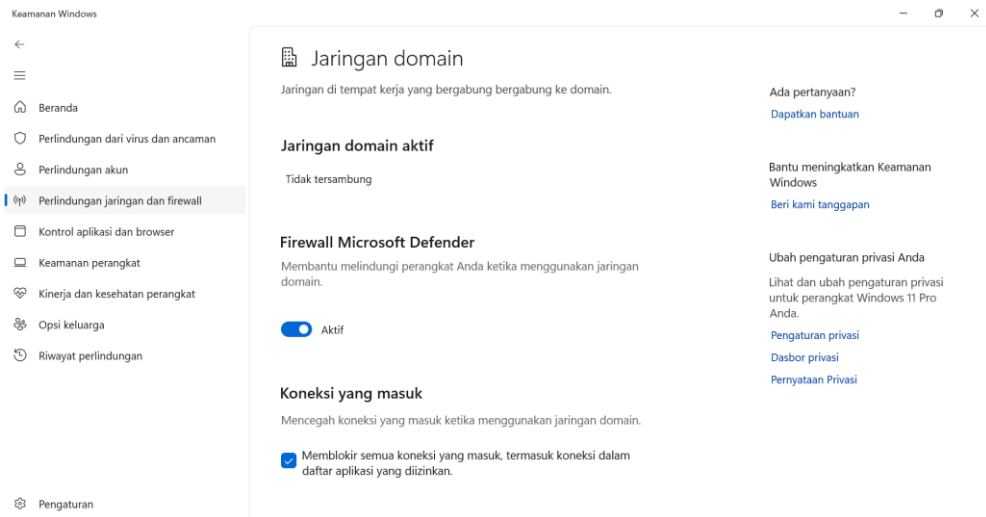
Dalam windows 11 ada 3 jenis fungsi firewall yang digunakan untuk melindunginya. Ketiga fungsi firewall tersebut adalah :

Jaringan Domain

Temuan penelitian menunjukkan bahwa jaringan domain berkaitan dengan lingkungan jaringan organisasi atau perusahaan. Dalam lingkungan tersebut, komputer biasanya terhubung dengan jaringan yang dikelola berdasarkan kebijakan keamanan organisasi. Oleh karena itu, penggunaan firewall pada jaringan domain tidak dapat dilepaskan dari kebijakan teknologi informasi yang diterapkan oleh organisasi. Hasil observasi dalam penelitian menunjukkan bahwa pada lingkungan perusahaan, firewall dapat dikelola secara terpusat oleh bagian teknologi informasi dan dapat menggunakan perangkat firewall tersendiri sesuai kebutuhan organisasi. Kondisi tersebut menunjukkan bahwa firewall bawaan Windows 11 tetap memiliki fungsi penting sebagai bagian dari mekanisme perlindungan komputer, tetapi penerapannya perlu disesuaikan dengan kebijakan keamanan jaringan organisasi. Dari sisi teori keamanan komputer, temuan pada jaringan domain memperlihatkan pentingnya pengelolaan keamanan secara terstruktur. Kurniawan dan Nugroho (2020) membahas penerapan keamanan jaringan komputer dengan pendekatan *layered security*, yang menunjukkan bahwa perlindungan sistem dapat dilakukan melalui beberapa lapisan keamanan. Dalam konteks penelitian ini, firewall pada Windows 11 dapat dipahami sebagai salah satu lapisan perlindungan tersebut. Namun, firewall komputer pengguna tidak dapat dipandang sebagai satu-satunya mekanisme keamanan, khususnya dalam jaringan

perusahaan yang memiliki sistem keamanan terpusat. Artinya, optimalisasi firewall pada Windows 11 akan lebih efektif apabila menjadi bagian dari kebijakan keamanan jaringan yang lebih luas. (Kurniawan & Nugroho, 2020; Buck et al., 2021; Ferretti et al., 2021).

Temuan tersebut juga memperlihatkan adanya hubungan antara konfigurasi teknis dan kebijakan keamanan organisasi. Pengguna pada jaringan domain tidak dapat melakukan pengaturan secara bebas apabila terdapat aturan yang telah ditentukan oleh administrator jaringan. Oleh sebab itu, optimalisasi firewall pada lingkungan domain harus mempertimbangkan kebutuhan akses, kebijakan perusahaan, dan sistem keamanan yang telah diterapkan. Hal ini memperkuat pandangan bahwa keamanan komputer tidak hanya bergantung pada teknologi yang digunakan, tetapi juga pada tata kelola dan pengelolaan sistem keamanan. (Kim et al., 2021; Lee et al., 2021; Alicea & Alsmadi, 2021).



Gambar 3 : Jaringan Domain

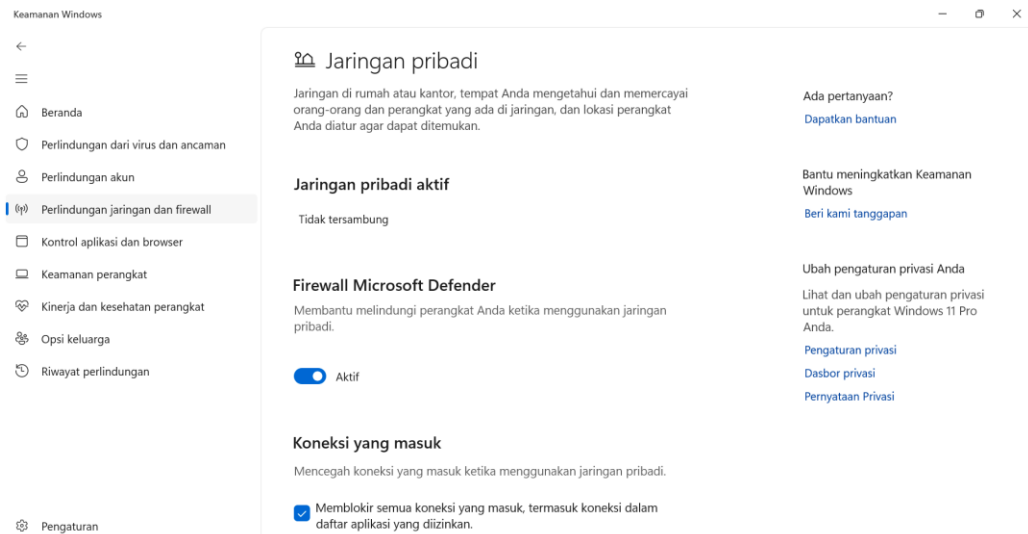
Perlu diingat bahwa di setiap perusahaan, penggunaan firewall ini mempunyai kebijakan tersendiri, karena biasanya perusahaan akan menggunakan firewall terpusat dalam jaringan perusahaan, biasanya berupa perangkat tersendiri yang disimpan dan dikelola oleh bagian Teknologi Informasi.

Jaringan Pribadi

Pada jaringan pribadi, hasil penelitian menunjukkan bahwa firewall memiliki fungsi preventif yang penting karena perangkat komputer atau perangkat digital dalam lingkungan rumah dapat terhubung ke internet secara terus-menerus. Lingkungan rumah dapat terdiri atas beberapa perangkat yang digunakan oleh anggota keluarga. Kondisi tersebut meningkatkan kebutuhan terhadap perlindungan sistem, terutama ketika perangkat digunakan untuk mengakses internet, bertukar data, atau menjalankan berbagai aplikasi. Oleh karena itu, aktivasi dan optimalisasi firewall pada jaringan pribadi dapat menjadi salah satu langkah awal untuk mengurangi risiko gangguan keamanan. (Beaman et al., 2021; McIntosh et al., 2021).

Temuan ini dapat diinterpretasikan melalui konsep keamanan komputer yang menempatkan pencegahan sebagai salah satu aspek penting dalam melindungi data dan sistem. Chowdhury et al. (2020) menjelaskan keamanan komputer sebagai bidang yang berkaitan dengan perlindungan sistem dan informasi dari berbagai ancaman. Dalam konteks Windows 11, firewall dapat menjadi mekanisme preventif yang bekerja sebelum gangguan atau akses tidak diinginkan terjadi. Dengan demikian, penggunaan firewall pada jaringan pribadi menunjukkan bahwa keamanan tidak hanya diperlukan dalam lingkungan perusahaan, tetapi juga dalam lingkungan rumah yang terhubung dengan internet. (Chowdhury et al., 2020; Hidayat & Prasetyo, 2021).

Hasil penelitian juga memperlihatkan bahwa pengguna rumahan perlu memiliki pemahaman mengenai fungsi firewall. Keberadaan firewall sebagai fitur bawaan Windows 11 tidak secara otomatis menjamin bahwa seluruh sistem telah terlindungi secara optimal. Pengguna tetap perlu mengetahui jenis jaringan yang digunakan, fungsi pengaturan firewall, serta kondisi akses jaringan yang diperbolehkan. Dengan demikian, faktor pengguna menjadi salah satu aspek penting dalam optimalisasi keamanan sistem. Hal tersebut sejalan dengan latar belakang penelitian yang menempatkan kelalaian dan keterbatasan pengetahuan pengguna sebagai salah satu persoalan dalam penerapan keamanan dasar pada sistem operasi Windows 11. (Ramdhani et al., 2026; Supriyanto et al., 2026).



Gambar 4 : Jaringan Pribadi

Jaringan Publik

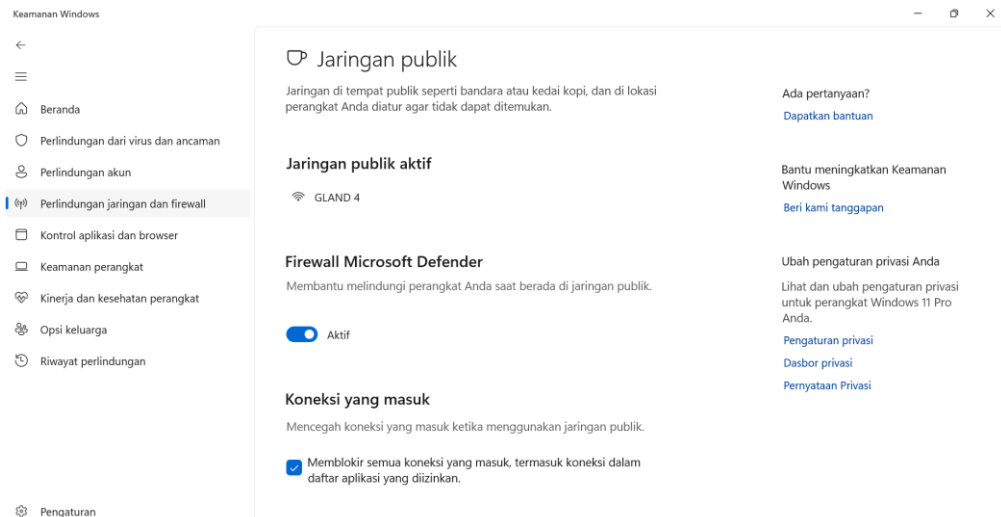
Jaringan publik adalah jaringan yang dapat diakses secara luas dan pada dasarnya tidak ada larangan untuk membatasi akses. Hal ini sangat berbahaya karena ada kemungkinan ada penyadapan dari pihak luar yang mengakibatkan kerusakan sistem atau kehilangan data. (Sengupta & Lakshminarayanan, 2021; Beaman et al., 2021).

Jaringan publik memberikan kenyamanan bagi pengguna karena bisa melakukan akses internet secara langsung tanpa harus menggunakan password, oleh karena untuk mencegah hal yang tidak diinginkan maka perlu cara untuk menghindarinya yaitu mengoptimalkan fungsi firewall yang sudah ada.

Temuan berikutnya berkaitan dengan jaringan publik. Penelitian menunjukkan bahwa jaringan publik memiliki tingkat risiko yang lebih tinggi dibandingkan jaringan pribadi karena jaringan tersebut dapat digunakan oleh banyak pengguna dan berada di luar kendali langsung pengguna komputer. Kondisi tersebut meningkatkan kemungkinan terjadinya akses atau komunikasi jaringan yang tidak diinginkan. Oleh karena itu, penggunaan firewall pada jaringan publik menjadi semakin penting sebagai salah satu mekanisme perlindungan preventif. (Alicia & Alsmadi, 2021; Khoumsi et al., 2018).

Dalam konteks ini, firewall berfungsi sebagai mekanisme pengawasan dan penyaringan lalu lintas data. Penggunaan firewall secara optimal dapat membantu membatasi lalu lintas jaringan berdasarkan pengaturan keamanan yang diterapkan. Temuan tersebut sesuai dengan konsep firewall yang dikemukakan Khoumsi et al. (2018), yaitu firewall berperan dalam memantau serta memisahkan lalu lintas yang berasal dari sumber yang dipercaya dan tidak dipercaya. Dengan demikian, semakin tinggi tingkat keterbukaan suatu jaringan, semakin penting pula penerapan mekanisme pengamanan terhadap lalu lintas data. (Kim et al., 2021; Lee et al., 2021).

Temuan pada jaringan publik juga memiliki kesesuaian dengan kajian Wicaksono (2022) mengenai sistem keamanan jaringan menggunakan firewall melalui *port blocking* dan *firewall filtering*. Kajian tersebut menunjukkan pentingnya pengendalian lalu lintas jaringan sebagai bagian dari perlindungan sistem. Dalam penelitian ini, fungsi firewall Windows 11 dapat dipahami dalam konteks yang serupa, yaitu sebagai mekanisme yang membantu mengontrol komunikasi jaringan. Perbedaannya, penelitian ini lebih menitikberatkan pada optimalisasi firewall bawaan Windows 11 dan penerapannya pada tiga profil jaringan, bukan pada pengujian metode *port blocking* atau *firewall filtering* tertentu. (Wicaksono, 2022; Liu et al., 2020; Yu & Bian, 2020).



Gambar 5 : Jaringan Publik

KESIMPULAN

Berdasarkan hasil penelitian mengenai optimalisasi penggunaan firewall dalam sistem operasi Windows 11, dapat disimpulkan bahwa firewall merupakan salah satu komponen penting dalam upaya meningkatkan keamanan dan perlindungan sistem terhadap berbagai ancaman siber. Firewall bawaan Windows 11 memiliki fungsi untuk mengawasi, mengontrol, dan menyaring lalu lintas data yang masuk dan keluar dari sistem sehingga dapat dimanfaatkan sebagai salah satu mekanisme keamanan preventif. Hasil penelitian menunjukkan bahwa keberadaan firewall bawaan pada Windows 11 memberikan fasilitas perlindungan yang dapat dioptimalkan oleh pengguna sesuai dengan kondisi dan karakteristik jaringan yang digunakan. (Khoumsi et al., 2018; Kim et al., 2021; Alicea & Alsmadi, 2021).

Optimalisasi firewall perlu memperhatikan tiga jenis profil jaringan, yaitu jaringan domain, jaringan pribadi, dan jaringan publik. Pada jaringan domain, penggunaan firewall perlu disesuaikan dengan kebijakan keamanan organisasi atau perusahaan. Pada jaringan pribadi, firewall dapat dimanfaatkan sebagai perlindungan preventif terhadap perangkat yang terhubung dalam lingkungan rumah. Sementara itu, pada jaringan publik yang memiliki tingkat keterbukaan lebih tinggi, optimalisasi firewall menjadi penting untuk membantu mengendalikan dan menyaring lalu lintas jaringan yang masuk dan keluar dari sistem. Dengan demikian, optimalisasi firewall tidak hanya berkaitan dengan keberadaan fitur tersebut, tetapi juga dengan pemahaman pengguna terhadap fungsi dan penerapannya sesuai dengan jenis jaringan. (Kurniawan & Nugroho, 2020; Buck et al., 2021; Ferretti et al., 2021).

Penelitian ini menjawab tujuan penelitian bahwa optimalisasi fungsi firewall bawaan Windows 11 dapat menjadi salah satu upaya preventif dalam menjaga keamanan sistem. Namun, firewall tidak dapat dipandang sebagai satu-satunya solusi keamanan karena perlindungan sistem juga membutuhkan penerapan keamanan lainnya secara terpadu. Implikasi penelitian ini adalah pentingnya meningkatkan pemahaman pengguna mengenai fungsi firewall dan konfigurasi keamanan Windows 11 agar fitur yang telah tersedia dapat dimanfaatkan secara optimal. (Mosteiro-Sanchez et al., 2020; McIntosh et al., 2021).

Penelitian selanjutnya disarankan untuk mengembangkan kajian ini melalui pengujian secara eksperimental dan terukur, misalnya dengan membandingkan kondisi sistem sebelum dan sesudah optimalisasi firewall atau menguji efektivitas konfigurasi firewall terhadap berbagai jenis ancaman siber. Pengembangan tersebut diperlukan agar efektivitas optimalisasi firewall pada Windows 11 dapat diketahui secara lebih objektif dan menghasilkan bukti empiris yang lebih kuat. (Liu et al., 2020; Yu & Bian, 2020; Ramdhani et al., 2026).

REFERENSI

1. Khoumsi, A., Erradi, M., & Krombi, W. (2018). A formal basis for the design and analysis of firewall security policies. *Journal of King Saud University - Computer and Information Sciences*, 30(1), 51–66. <https://doi.org/10.1016/j.jksuci.2016.11.008>

2. Hu, H., Han, W., Kyung, S., Wang, J., Ahn, G. J., Zhao, Z., & Li, H. (2019). Towards a reliable firewall for software-defined networks. *Computers & Security*, 87, 101597. <https://doi.org/10.1016/j.cose.2019.101597>
3. Li, D., Guo, H., Zhou, J., Zhou, L., & Wong, J. W. (2019). SCADAWall: A CPI-enabled firewall model for SCADA security. *Computers & Security*, 80, 134–154. <https://doi.org/10.1016/j.cose.2018.10.002>
4. Kim, T., Kwon, T., Lee, J., & Song, J. (2021). F/Wvis: Hierarchical visual approach for effective optimization of firewall policy. *IEEE Access*, 9, 105989–106004. <https://doi.org/10.1109/ACCESS.2021.3100141>
5. Lee, H., Lee, S., Kim, K., & Kim, H. K. (2021). HSViz: Hierarchy simplified visualizations for firewall policy analysis. *IEEE Access*, 9, 71737–71753. <https://doi.org/10.1109/ACCESS.2021.3077146>
6. Alicea, M., & Alsmadi, I. (2021). Misconfiguration in firewalls and network access controls: Literature review. *Future Internet*, 13(11), 283. <https://doi.org/10.3390/fi13110283>
7. Usman, M., Jan, M. A., He, X., & Chen, J. (2019). A survey on representation learning efforts in cybersecurity domain. *ACM Computing Surveys*, 52(6), 111, 1–28. <https://doi.org/10.1145/3331174>
8. Liu, C., Liu, Y., Yan, Y., & Wang, J. (2020). An intrusion detection model with hierarchical attention mechanism. *IEEE Access*, 8, 67542–67554. <https://doi.org/10.1109/ACCESS.2020.2983568>
9. Yu, Y., & Bian, N. (2020). An intrusion detection method using few-shot learning. *IEEE Access*, 8, 49730–49740. <https://doi.org/10.1109/ACCESS.2020.2980136>
10. Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, 97, 101963. <https://doi.org/10.1016/j.cose.2020.101963>
11. Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieto, A. (2020). Securing IIoT using defence-in-depth: Towards an end-to-end secure Industry 4.0. *Journal of Manufacturing Systems*, 57, 367–378. <https://doi.org/10.1016/j.jmsy.2020.10.011>
12. Alexander, R. (2020). Reducing threats by using Bayesian networks to prioritize and combine defense in depth security measures. *Journal of Information Security*, 11(3), 121–137. <https://doi.org/10.4236/jis.2020.113008>
13. Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, 110, 102436. <https://doi.org/10.1016/j.cose.2021.102436>
14. Ferretti, L., Magnanini, F., Andreolini, M., & Colajanni, M. (2021). Survivable zero trust for cloud computing environments. *Computers & Security*, 110, 102419. <https://doi.org/10.1016/j.cose.2021.102419>
15. McIntosh, T., Kayes, A. S. M., Chen, Y.-P. P., Ng, A., & Watters, P. (2021). Dynamic user-centric access control for detection of ransomware attacks. *Computers & Security*, 111, 102461. <https://doi.org/10.1016/j.cose.2021.102461>
16. Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, 111, 102490. <https://doi.org/10.1016/j.cose.2021.102490>
17. Wicaksono, D. (2022). Sistem keamanan jaringan dengan menggunakan firewall dengan metode port blocking dan firewall filtering. *Jurnal Teknik Informatika dan Sistem Informasi*, 9(2).
18. Kurniawan, D., & Nugroho, A. (2020). Implementasi keamanan jaringan komputer menggunakan metode layered security. *Jurnal Sistem Informasi*, 16(1), 33–41.
19. Hidayat, R., & Prasetyo, Y. (2021). Analisis keamanan sistem informasi berbasis manajemen risiko teknologi informasi. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 8(2), 245–252.
20. Dwinanto, & Setiyani, H. (2021). Implementasi keamanan komputer pada aspek confidentiality, integrity, availability (CIA) menggunakan tools Lynis Audit System. *Jurnal Maklumatika*, 8(1), 35–46.
21. Pratama, I. P. A. E. (2018). Analisis ancaman keamanan sistem operasi pada lingkungan teknologi informasi modern. *Jurnal Nasional Teknologi dan Sistem Informasi*, 4(3), 120–128.
22. Ramdhani, M. S. N., Tahir, M., & Alhaq, M. M. (2026). Pengembangan sistem Intrusion Detection and Prevention System (IDPS) berbasis Random Forest dan Windows Defender Firewall pada jaringan lokal testing. *Jurnal Komputer Teknologi Informasi Sistem Komputer*, 5(1), 613–619. <https://doi.org/10.62712/juktisi.v5i1.1054>
23. Supriyanto, S., Kannajmi, A. R., & Saputra, D. (2026). Evaluasi efektivitas hardening dalam meningkatkan keamanan sistem operasi Windows dan Linux. *Jurnal Informatika dan Sistem Informasi UNTIRTA*, 1(1).

24. Hadi, R., Abdullah, R. K., & Fitriani, H. P. (2026). Penerapan firewall dan intrusion detection system pada jaringan komputer. *Journal of Computer Science and Information Technology*, 2(1). <https://doi.org/10.70716/jocsit.v2i1.411>
25. Sengupta, B., & Lakshminarayanan, A. (2021). DistriTrust: Distributed and low-latency access validation in zero-trust architecture. *Journal of Information Security and Applications*, 63, 103023. <https://doi.org/10.1016/j.jisa.2021.103023>