

Penerapan Firewall dan Intrusion Detection System pada Jaringan Komputer

Ronal Hadi^{a,1,*}, Riska Kurniyanto Abdullah^{b,2}, Harry Pribadi Fitrian^{c,3},

^a Program Studi Sistem Informasi, Institut Teknologi Kalimantan, Balikpapan, Indonesia

^b Program Studi Teknik Informatika, Universitas Tanjungpura, Pontianak, Indonesia

^c Program Studi Teknologi Informasi, Universitas Lambung Mangkurat, Banjarmasin, Indonesia

¹ ronalhadi@gmail.com*; ² riskakabdullah@gmail.com; ³ harrypf@gmail.com;

* Corresponding author

ARTICLE INFO

Article history

Received 20 February 2026

Revised 25 February 2026

Accepted 23 March 2026

Published 25 March 2026

Keywords

firewall
intrusion detection system
network security
cyber attack
server protection



License by CC-BY-SA

Copyright © 2026, The Author(s).

ABSTRACT

Network security has become a critical aspect as organizations increasingly rely on network-based information systems. Firewalls, as the first line of defense, have limitations in detecting complex and dynamic cyber attacks. Therefore, integrating Intrusion Detection Systems (IDS) is widely adopted to enhance network resilience. This study aims to analyze the implementation of firewalls and IDS in improving computer network security based on literature review and implementation studies. The research method employs a descriptive-analytical approach through a systematic literature review and comparative analysis of previous studies. The results indicate that the integration of firewalls and IDS significantly improves attack detection rates, accelerates security response, and reduces the risks of data breaches and service disruptions. IDS technologies such as Snort, OSSEC, and Suricata have proven effective in detecting brute force attacks, malware, and Distributed Denial of Service (DDoS) attacks when combined with firewall systems. This study concludes that the integrated implementation of firewalls and IDS is an effective and relevant strategy for securing modern computer networks.

How to cite: Hadi, R., Abdullah, R. K., & Fitrian, H. P. (2026). Penerapan Firewall dan Intrusion Detection System pada Jaringan Komputer. *Journal of Computer Science and Information Technology*, Vol 2(1), 09-15. doi: <https://doi.org/10.70716/jocsit.v2i1.411>

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan pemanfaatan jaringan komputer sebagai infrastruktur utama dalam penyelenggaraan layanan digital. Jaringan komputer digunakan secara luas pada sektor pemerintahan, pendidikan, industri, dan layanan publik untuk mendukung pertukaran data, pengelolaan sistem informasi, serta operasional berbasis internet. Namun, peningkatan ketergantungan terhadap jaringan komputer juga diikuti oleh meningkatnya risiko ancaman keamanan siber yang semakin kompleks dan beragam. Ancaman tersebut meliputi serangan malware, brute force attack, Distributed Denial of Service (DDoS), serta eksploitasi celah keamanan sistem yang dapat mengakibatkan gangguan layanan, kebocoran data, dan kerugian organisasi secara signifikan (Hadi et al., 2022; Fitrian et al., 2025).

Firewall merupakan mekanisme keamanan jaringan yang berfungsi sebagai pengendali lalu lintas data antara jaringan internal dan jaringan eksternal berdasarkan aturan tertentu. Firewall mampu memfilter paket data, mengatur hak akses, serta memblokir lalu lintas yang tidak sesuai dengan kebijakan keamanan yang telah ditetapkan. Penelitian terdahulu menunjukkan bahwa firewall efektif dalam mencegah akses tidak sah dan mengurangi risiko serangan dari luar jaringan (Zhang et al., 2024; Naedele et al., 2006). Namun demikian, firewall tradisional memiliki keterbatasan dalam mendeteksi serangan yang bersifat kompleks, terutama serangan yang berasal dari dalam jaringan atau serangan yang memanfaatkan celah aplikasi dan perilaku abnormal pengguna (Wu, n.d.; Zhang, 2008).

Keterbatasan firewall tersebut mendorong pengembangan dan penerapan Intrusion Detection System (IDS) sebagai mekanisme keamanan tambahan. IDS dirancang untuk mendeteksi aktivitas mencurigakan

dengan menganalisis pola lalu lintas jaringan, log sistem, dan perilaku pengguna. IDS mampu mengidentifikasi serangan yang tidak dapat dideteksi oleh firewall, seperti serangan berbasis signature maupun anomaly-based intrusion (Widodo & Aji, 2021; Abdullah et al., 2024). Dengan kemampuan deteksi secara real-time, IDS memberikan peringatan dini kepada administrator jaringan sehingga respons terhadap ancaman dapat dilakukan lebih cepat dan terarah.

Berbagai penelitian menunjukkan bahwa integrasi firewall dan IDS memberikan tingkat perlindungan yang lebih tinggi dibandingkan penerapan firewall secara mandiri. Wang dan Yan (2015) menyatakan bahwa kombinasi firewall dan IDS pada jaringan kampus mampu meningkatkan intensitas deteksi intrusi serta mengendalikan akses data secara lebih efektif. Temuan serupa juga disampaikan oleh Xie et al. (2012) dan Ashfaq et al. (2004), yang menegaskan bahwa sistem keamanan terpadu memungkinkan pembaruan kebijakan keamanan secara dinamis berdasarkan hasil deteksi IDS, sehingga meningkatkan ketahanan jaringan terhadap serangan yang terus berkembang.

Implementasi IDS berbasis open-source seperti Snort, OSSEC, dan Suricata banyak diterapkan pada lingkungan server dan jaringan skala menengah hingga besar. Hadi et al. (2022) menunjukkan bahwa OSSEC mampu meningkatkan keamanan server melalui analisis log, pemeriksaan integritas file, dan deteksi rootkit. Sementara itu, penelitian Abdullah et al. (2024) dan Widiyanto dan Sulisty (2021) membuktikan bahwa penggunaan Snort yang dikombinasikan dengan firewall seperti iptables efektif dalam mendeteksi dan mencegah serangan brute force dan DDoS. Temuan ini menunjukkan bahwa IDS berperan penting dalam melengkapi fungsi firewall dalam menjaga keamanan jaringan komputer.

Selain meningkatkan kemampuan deteksi, integrasi firewall dan IDS juga memberikan manfaat dalam aspek pemantauan dan manajemen keamanan jaringan. Penelitian Alfariy et al. (2025) mengungkapkan bahwa penggunaan sistem IDS hibrida yang dikombinasikan dengan manajemen log terpusat mampu meningkatkan visibilitas aktivitas jaringan dan mempercepat proses analisis insiden keamanan. Sistem ini memungkinkan administrator jaringan untuk melakukan pemantauan secara menyeluruh dan mengambil keputusan berbasis data yang lebih akurat. Dengan demikian, penerapan firewall dan IDS tidak hanya berfungsi sebagai mekanisme pencegahan, tetapi juga sebagai alat pendukung pengambilan keputusan dalam manajemen keamanan jaringan.

Meskipun manfaat integrasi firewall dan IDS telah banyak dilaporkan, implementasinya masih menghadapi sejumlah tantangan. Kompleksitas konfigurasi, kebutuhan sumber daya sistem yang tinggi, serta potensi terjadinya false positive menjadi kendala yang sering ditemui dalam penerapan IDS pada lingkungan operasional (Luan, 2007; Zhang, 2008). Selain itu, efektivitas sistem keamanan sangat bergantung pada pembaruan aturan dan kebijakan keamanan yang berkelanjutan agar mampu menghadapi pola serangan baru yang terus berkembang (Zhang & Luo, 2023).

Berdasarkan uraian tersebut, dapat disimpulkan bahwa penerapan firewall dan Intrusion Detection System secara terpadu merupakan kebutuhan yang mendesak dalam menjaga keamanan jaringan komputer modern. Namun, diperlukan pemahaman yang komprehensif mengenai peran, kelebihan, dan keterbatasan masing-masing sistem agar integrasi yang diterapkan dapat berjalan secara optimal. Oleh karena itu, penelitian ini bertujuan untuk menganalisis penerapan firewall dan IDS dalam meningkatkan keamanan jaringan komputer berdasarkan kajian literatur dan hasil implementasi terdahulu. Kontribusi penelitian ini diharapkan dapat memberikan gambaran sistematis mengenai efektivitas sistem keamanan terpadu serta menjadi referensi bagi pengelola jaringan dalam merancang strategi keamanan yang lebih andal dan berkelanjutan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif-analitis dengan tujuan untuk menganalisis penerapan firewall dan Intrusion Detection System (IDS) dalam meningkatkan keamanan jaringan komputer. Pendekatan ini dipilih karena sesuai untuk mengkaji, membandingkan, dan mengevaluasi karakteristik, fungsi, serta efektivitas sistem keamanan jaringan berdasarkan bukti empiris yang telah dilaporkan dalam penelitian sebelumnya. Penelitian tidak berfokus pada pengujian hipotesis baru, melainkan pada pemaparan dan analisis sistematis terhadap praktik penerapan firewall dan IDS yang telah diterapkan pada berbagai lingkungan jaringan.

Desain dan Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian kepustakaan (library research) dengan desain analisis komparatif. Penelitian ini menelaah berbagai hasil penelitian yang relevan mengenai penerapan

firewall dan IDS pada jaringan komputer, baik pada lingkungan server, jaringan kampus, maupun infrastruktur jaringan organisasi. Desain ini memungkinkan peneliti untuk mengidentifikasi pola penerapan, kelebihan, serta keterbatasan integrasi firewall dan IDS berdasarkan temuan empiris yang telah dipublikasikan sebelumnya.

Sumber dan Teknik Pengumpulan Data

Data penelitian diperoleh dari sumber sekunder berupa artikel jurnal ilmiah nasional dan internasional terakreditasi, prosiding konferensi ilmiah, serta dokumen teknis yang membahas implementasi firewall dan intrusion detection system. Seluruh sumber data yang digunakan telah tercantum dalam daftar pustaka penelitian dan dipilih berdasarkan relevansi topik, keterkinian publikasi, serta kesesuaian konteks penelitian dengan keamanan jaringan komputer. Teknik pengumpulan data dilakukan melalui penelusuran, seleksi, dan pengelompokan literatur yang membahas firewall, IDS, serta integrasi keduanya dalam sistem keamanan jaringan.

Objek dan Fokus Analisis

Objek penelitian ini adalah sistem keamanan jaringan komputer yang menerapkan firewall dan IDS secara terpadu. Fokus analisis diarahkan pada beberapa aspek utama, yaitu fungsi firewall dalam mengendalikan lalu lintas jaringan, peran IDS dalam mendeteksi intrusi, serta efektivitas integrasi kedua sistem dalam meningkatkan keamanan jaringan. Selain itu, penelitian ini juga menganalisis jenis serangan yang dapat dideteksi, mekanisme respons keamanan, serta implikasi penerapan sistem keamanan terpadu terhadap pengelolaan jaringan.

Teknik Analisis Data

Analisis data dilakukan secara kualitatif deskriptif dengan tahapan sebagai berikut. Pertama, dilakukan identifikasi dan klasifikasi hasil penelitian terdahulu berdasarkan jenis sistem keamanan yang diterapkan, seperti firewall tradisional, IDS berbasis Snort, OSSEC, dan Suricata. Kedua, dilakukan analisis komparatif terhadap hasil penelitian untuk mengidentifikasi persamaan dan perbedaan temuan terkait efektivitas sistem keamanan jaringan. Ketiga, hasil analisis disintesis untuk memperoleh gambaran menyeluruh mengenai penerapan firewall dan IDS serta kontribusinya terhadap peningkatan keamanan jaringan komputer.

Validitas dan Keandalan Analisis

Untuk menjaga validitas dan keandalan analisis, penelitian ini hanya menggunakan sumber yang telah melalui proses peer-review dan diterbitkan pada jurnal atau prosiding ilmiah yang kredibel. Selain itu, konsistensi temuan antarpengelitian dianalisis untuk memastikan bahwa kesimpulan yang diambil didukung oleh lebih dari satu sumber. Pendekatan ini bertujuan untuk meminimalkan bias interpretasi serta menjaga objektivitas dalam analisis hasil penelitian.

Batasan Penelitian

Penelitian ini memiliki batasan pada penggunaan data sekunder tanpa melakukan pengujian langsung pada lingkungan jaringan tertentu. Oleh karena itu, hasil penelitian merefleksikan kondisi dan temuan yang dilaporkan dalam literatur yang dianalisis. Meskipun demikian, pendekatan ini tetap relevan untuk memberikan gambaran komprehensif mengenai penerapan firewall dan IDS serta menjadi dasar bagi penelitian lanjutan yang bersifat eksperimental atau implementatif.

HASIL DAN PEMBAHASAN

Hasil analisis menunjukkan bahwa firewall berfungsi sebagai mekanisme kontrol akses jaringan dengan menyaring lalu lintas data berdasarkan kebijakan keamanan yang telah ditetapkan. Firewall efektif dalam mencegah akses tidak sah dari jaringan eksternal serta membatasi komunikasi jaringan berdasarkan aturan port, protokol, dan alamat IP. Namun, firewall tidak mampu mendeteksi pola serangan kompleks yang memanfaatkan celah aplikasi atau perilaku abnormal pengguna internal (Zhang et al., 2024; Naedele et al., 2006). Temuan ini konsisten dengan penelitian Wu yang menyatakan bahwa firewall memiliki keterbatasan dalam mendeteksi intrusi berbasis perilaku dan serangan zero-day (Wu, n.d.).

Integrasi Intrusion Detection System (IDS) terbukti meningkatkan kemampuan sistem keamanan jaringan dalam mendeteksi aktivitas mencurigakan secara real-time. Penelitian Hadi et al. (2022) menunjukkan bahwa OSSEC mampu melakukan analisis log sistem, pemeriksaan integritas file, serta deteksi

rootkit pada server. Sementara itu, Abdullah et al. (2024) dan Widiyanto dan Sulisty (2021) melaporkan bahwa Snort yang dikombinasikan dengan firewall mampu mendeteksi serangan brute force dan DDoS dengan tingkat respons yang cepat. Hal ini menunjukkan bahwa IDS berperan sebagai lapisan keamanan tambahan yang melengkapi keterbatasan firewall.

Selain itu, penelitian Wang dan Yan (2015) serta Xie et al. (2012) menunjukkan bahwa sistem keamanan terpadu berbasis firewall dan IDS mampu meningkatkan intensitas deteksi intrusi serta memperkuat kontrol akses data pada jaringan kampus dan organisasi. Integrasi ini memungkinkan pembaruan kebijakan keamanan secara dinamis berdasarkan hasil deteksi IDS, sehingga meningkatkan ketahanan jaringan terhadap ancaman yang terus berkembang. Penelitian Ashfaq et al. (2004) juga menunjukkan bahwa integrasi firewall dan IDS dalam arsitektur jaringan berperforma tinggi dapat meningkatkan kemampuan deteksi ancaman secara real-time.

Penelitian Alfarisy et al. (2025) menunjukkan bahwa penggunaan sistem IDS hibrida yang dikombinasikan dengan manajemen log terpusat memberikan peningkatan signifikan dalam monitoring jaringan. Sistem ini memungkinkan visualisasi log serangan dan analisis pola intrusi secara komprehensif, sehingga mempercepat proses respons keamanan. Temuan ini menegaskan bahwa integrasi firewall dan IDS tidak hanya berfungsi sebagai mekanisme proteksi, tetapi juga sebagai alat monitoring dan analisis keamanan jaringan.

Meskipun demikian, beberapa penelitian juga mengidentifikasi tantangan dalam implementasi sistem keamanan terpadu. Luan (2007) dan Zhang (2008) menyatakan bahwa kompleksitas konfigurasi dan tingginya tingkat false positive dapat mengurangi efektivitas IDS jika tidak dikelola dengan baik. Selain itu, efektivitas sistem sangat bergantung pada pembaruan aturan keamanan dan kebijakan firewall yang berkelanjutan untuk menghadapi pola serangan baru yang terus berkembang (Zhang et al., 2023).

Tabel 1. Sintesis Hasil Penelitian Penerapan Firewall dan IDS

Peneliti	Sistem Keamanan	Temuan Utama
Hadi et al. (2022)	Firewall + OSSEC	Deteksi log, integritas file, dan rootkit pada server
Abdullah et al. (2024)	Snort + Fail2Ban	Deteksi brute force dan notifikasi serangan
Widiyanto & Sulisty (2021)	Snort + iptables	Pencegahan serangan DDoS dan aktivitas mencurigakan
Wang & Yan (2015)	Firewall + IDS	Peningkatan kontrol akses dan intensitas deteksi intrusi
Xie et al. (2012)	Distributed firewall + IDS	Pembaruan kebijakan keamanan dinamis
Alfarisy et al. (2025)	Hybrid IDS + Elastic Stack	Monitoring log terpusat dan analisis serangan

Tabel 2. Perbandingan Fungsi Firewall dan IDS

Aspek	Firewall	Intrusion Detection System
Fungsi utama	Kontrol akses jaringan	Deteksi intrusi
Teknik kerja	Filtering paket dan aturan kebijakan	Analisis signature dan anomaly
Keterbatasan	Tidak mendeteksi serangan internal kompleks	Potensi false positive
Peran dalam keamanan terpadu	Lapisan proteksi pertama	Lapisan deteksi dan respons



Gambar 1. Arsitektur Integrasi Firewall dan IDS pada Jaringan Komputer

Keterangan: Firewall berfungsi sebagai lapisan kontrol akses, IDS mendeteksi intrusi pada lalu lintas jaringan, dan sistem manajemen log digunakan untuk analisis serta respons keamanan.

Pembahasan Konseptual

Hasil sintesis penelitian menunjukkan bahwa firewall dan IDS memiliki peran yang saling melengkapi dalam sistem keamanan jaringan. Firewall berfungsi sebagai mekanisme pencegahan awal, sedangkan IDS berfungsi sebagai mekanisme deteksi dan respons. Integrasi kedua sistem ini menghasilkan pendekatan pertahanan berlapis (*defense in depth*) yang mampu meningkatkan ketahanan jaringan terhadap berbagai ancaman siber.

Temuan ini sejalan dengan model pertahanan jaringan yang menggabungkan firewall dan intrusion prevention system untuk meningkatkan efektivitas perlindungan sistem informasi (Wu, n.d.; Zhang et al., 2024). Selain itu, penerapan sistem keamanan terdistribusi juga memungkinkan pengelolaan kebijakan keamanan secara adaptif dan real-time (Xie et al., 2012).

Secara praktis, hasil penelitian ini menunjukkan bahwa organisasi perlu mengintegrasikan firewall dan IDS dalam infrastruktur jaringan untuk meningkatkan keamanan sistem. Selain itu, pembaruan aturan keamanan dan pemantauan log secara berkala menjadi faktor kunci dalam menjaga efektivitas sistem keamanan jaringan.

KESIMPULAN

Penelitian ini menyimpulkan bahwa penerapan firewall dan Intrusion Detection System (IDS) secara terpadu merupakan pendekatan yang efektif dalam meningkatkan keamanan jaringan komputer. Firewall berperan sebagai mekanisme pengendali akses yang menyaring lalu lintas jaringan berdasarkan kebijakan keamanan, sedangkan IDS berfungsi sebagai sistem pendeteksi intrusi yang mampu mengidentifikasi aktivitas mencurigakan secara real-time. Integrasi kedua sistem tersebut memungkinkan terbentuknya mekanisme pertahanan berlapis yang mampu mengatasi keterbatasan masing-masing sistem ketika diterapkan secara terpisah.

Hasil analisis menunjukkan bahwa penggunaan IDS berbasis Snort, OSSEC, dan Suricata yang dikombinasikan dengan firewall mampu meningkatkan kemampuan deteksi terhadap berbagai jenis serangan, seperti brute force attack, malware, dan Distributed Denial of Service (DDoS). Selain itu, sistem keamanan terpadu juga mendukung pemantauan aktivitas jaringan secara lebih komprehensif melalui analisis log dan visualisasi data, sehingga mempercepat proses respons terhadap insiden keamanan. Temuan ini menegaskan bahwa IDS tidak hanya berfungsi sebagai alat deteksi, tetapi juga sebagai komponen penting dalam manajemen keamanan jaringan.

Meskipun demikian, efektivitas penerapan firewall dan IDS sangat bergantung pada konfigurasi sistem, pembaruan aturan keamanan, serta pengelolaan log yang berkelanjutan. Kompleksitas konfigurasi dan potensi terjadinya false positive menjadi tantangan yang perlu dikelola secara sistematis agar tidak mengurangi kinerja sistem keamanan. Oleh karena itu, organisasi disarankan untuk menerapkan kebijakan keamanan yang adaptif dan melakukan evaluasi berkala terhadap sistem firewall dan IDS yang digunakan.

Secara keseluruhan, penelitian ini memberikan kontribusi dalam memperkuat pemahaman mengenai pentingnya integrasi firewall dan IDS sebagai strategi keamanan jaringan komputer. Penelitian selanjutnya disarankan untuk mengkaji aspek implementasi teknis secara lebih mendalam pada lingkungan jaringan tertentu guna meningkatkan efektivitas dan efisiensi sistem keamanan jaringan.

DAFTAR PUSTAKA

- Abdullah, R. K., Fudhail, M., & Mujahidin, S. (2024). Penggunaan Snort dan Fail2Ban sebagai IDS untuk mengatasi brute force attack dengan notifikasi Telegram: Studi kasus pada institusi XYZ. *Jurnal Sistem dan Teknologi Informasi (JustIN)*, 12(3). <https://doi.org/10.26418/justin.v12i3.79617>
- Agustin, R., Fitri, I., & Nathasia, N. D. (2018). Implementasi metode intrusion detection systems (IDS) dan intrusion prevention systems (IPS) berbasis Snort server untuk keamanan jaringan LAN. *Jurnal Informatika*, 18(1). <https://doi.org/10.30873/JI.V18i1.1118>
- Ashfaq, O., Mairaj, J., Raza, A., & Khan, S. (2004). Field upgradeable, dynamically reconfigurable accelerated firewall for networks. *Proceedings of the International Conference on Security of Networks (SCONES)*. <https://doi.org/10.1109/SCONES.2004.1564786>
- Durahman, Y., Nanang, H., & Arifin, V. (2024). Anticipating computer security using the Snort intrusion detection system. *Proceedings of the 6th International Conference on Cyber and IT Service Management (CITSM)*. <https://doi.org/10.1109/citsm64103.2024.10775522>
- Fitrian, H. P., Noorjamil, B. F., & Rahmawati, F. (2025). Analisis efektivitas firewall dalam memfilter dan melindungi lalu lintas jaringan. *Jurnal Nasional Komputasi dan Teknologi Informasi*, 8(1). <https://doi.org/10.32672/jnkti.v8i1.8554>
- Hadi, R., Yuliana, Y., & Mooduto, H. A. (2022). Deteksi ancaman keamanan pada server dan jaringan menggunakan OSSEC. *Jurnal Ilmiah Teknologi Sistem Informasi*, 3(1). <https://doi.org/10.30630/jitsi.3.1.58>
- Hadi, R., Yuliana, Y., & Mooduto, H. A. (2022). Deteksi ancaman keamanan pada server dan jaringan menggunakan OSSEC. *Jurnal Ilmiah Teknologi Sistem Informasi*, 3(1). <https://doi.org/10.62527/jitsi.3.1.58>
- Hendrawan, R., Widyawati, L., & Asroni, O. (2025). Implementation of multihomed firewall based on IDS and DMZ technology using pfSense. *Journal of Artificial Intelligence and Engineering Applications*, 4(3). <https://doi.org/10.59934/jaiea.v4i3.1028>
- Lu, L. (2012). Joint distributed firewall and intrusion detection for network security protection system. *Modern Computer*.
- Luan, Z.-Y. (2007). Research and implementation of an integrated intrusion prevention system. *Information Technology*.
- Luan, Z.-Y. (2007). Research and implementation of an integrated intrusion prevention system. <https://doi.org/10.3969/j.issn.1009-2552.2007.12.047>
- Naedele, M., Dzung, D., & Sager, P. (2006). *Firewall and intrusion detection system* (Patent).
- Widodo, T., & Aji, A. S. (2021). Implementation of intrusion detection system (IDS) and Snort community rules to detect types of network attacks. *International Journal of Computer Applications*. <https://doi.org/10.5120/ijca2021921821>
- Wu, D. (n.d.). Research on network security defense model based on combination strategy of firewall and IPS. <https://doi.org/10.17762/jfcr.vi.215>
- Wang, J., & Yan, P. (2015). Analysis on the application of campus network firewall and intrusion detection system. *Proceedings of ISRME*. <https://doi.org/10.2991/ISRME-15.2015.85>
- Wang, L.-H., Li, T., Zhang, X.-P., et al. (2006). An Internet intrusion detection system cooperating with firewall. <https://doi.org/10.3969/j.issn.1001-3695.2006.03.032>
- Xie, L., Yu, F., & Xu, C. (2012). Distributed firewall with intrusion detection system. *Journal of Computers*, 7(12), 3110–3115. <https://doi.org/10.4304/JCP.7.12.3110-3115>
- Zhang, M., Zhang, P., & Tang, X. (2024). Application of firewall technology in computer network information security. *Applied Information Technology Research*, 2(3). <https://doi.org/10.18686/aitr.v2i3.4404>
- Zhang, X., Luo, Z., & Zhang, J. (2023). Analysis of the application of firewall and intrusion detection technology in network security in the era of big data. *Proceedings of JCICE*. <https://doi.org/10.1109/jcice59059.2023.00042>
- Zhang, Y. (2012). Firewall and IDS linkage of network security technology application research. <https://doi.org/10.3969/j.issn.1009-3044.2012.13.042>
- 张晶. (2008). Application of intrusion detection in firewall system. <https://doi.org/10.3969/j.issn.1671-0428.2008.05.012>

- 李信满, 赵宏, & 马士军. (2001). Firewall-based intrusion detection system.
<https://doi.org/10.3321/j.issn:1005-3026.2001.05.005>
- 路莹. (2009). Research on the joint application of firewall and intrusion detect system.
<https://doi.org/10.3969/j.issn.1671-3982.2009.01.023>