Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 1, May 2025
https://doi.org/10.47709/brilliance.v5i1.6162

Firewall Implementation as a Computer Network Security Strategy for Data Protection

Fauzan Prasetyo Eka Putra[1*], Mohammat Dafid[2], Imam Syafi'i[3]
[1,2,3] Fakultas Teknik, Informatika, Universitas Madura, Pamekasan, Indonesia
[1]prasetyo@unira.ac.id, [2]mohammatdavid2023@gmail.com,[3]iimamsyafii111@gmail.com

***Corresponding Author**

Article History:
Submitted: 19-06-2025
Accepted: 23-06-2025
Published: 01-07-2025

Keywords:
Network Security; Firewall; Computer Network; Data Protection.

ABSTRACT

Computer network security plays a crucial role in ensuring the integrity, confidentiality, and availability of data in the modern digital era. One of the primary tools used to safeguard networks from unauthorized access and external threats is the firewall. This paper explores the significance of firewalls in protecting network systems by examining their functions, various types, and capability to regulate data traffic. Firewalls work by enforcing specific rules to limit access, effectively reducing the risk of cyber threats such as malware, hacking attempts, and unauthorized intrusions. The study also involves practical observation of firewall implementation in a real network setup to evaluate their efficiency in mitigating security risks. Findings indicate that properly configured firewalls can considerably strengthen a network's defense. Nevertheless, relying solely on firewalls is insufficient. They should be supported by additional security technologies and best practices to achieve comprehensive network protection. In conclusion, firewalls are essential elements in upholding the reliability and safety of computer networks.

INTRODUCTION

In the current global era, Information Technology (IT) has experienced rapid advancements, particularly with the rise of internet connectivity that facilitates communication among various stakeholders. Within the industrial sector, highly sensitive information is often at risk of exposure to unauthorized individuals (Saputra, 2023; Subakti, 2023).

As platforms that provide services and respond to HTTP requests, web servers are among the most vulnerable components to cyberattacks. Common threats targeting web servers include port scanning, brute force attacks, and distributed denial-of-service (DDoS) attacks (Anggraeni, Ginting, & Ikhwan, 2022; Innuddin, Irfan, & Hammad, 2023; Yuliandari et al., 2023; Hilmi & Khujaemah, 2022). In response to these vulnerabilities, this study proposes the development of a computer network security system for the Faculty of Information Technology at SWCU, utilizing a topology based on hierarchical network design. By adopting this approach, the goal is to establish a more organized and secure network architecture that aligns with structured design principles (Fauzan Prasetyo Eka Putra et al., 2024; Haidar et al., 2021).

Network security threats can originate from both internal and external users, especially when a local area network (LAN) is connected to the broader public internet. Such connections significantly increase the likelihood of unauthorized access and cyberattacks on system resources (Nurbahri & Nurcahyo, 2023; Rokhman et al., 2023; Sartomo & Sulistyo, 2022). To address these risks, effective network management becomes a critical responsibility for network administrators. They must actively oversee and monitor internet usage within the local network. Proper management practices not only reduce potential security threats but also help maintain an efficient and secure network infrastructure (Eben, Mukramin, & Abduh, 2024; Syahab, 2023).

There are various types of cyberattacks, with some of the most frequently encountered being Cross-Site Scripting (XSS), Distributed Denial of Service (DDoS), and SQL Injection. XSS, in particular, is considered highly dangerous due to its ease of execution. Numerous freely available tools enable even individuals with minimal hacking expertise to carry out such attacks effectively, making XSS a serious threat to web applications (Prasetyo, Haeruddin, & ..., 2024; Permana & Mitro, 2023; Diansyah, 2024; Syamsu & Widodo, 2022). Without appropriate security measures, organizations face the risk of data breaches and loss of critical information. Therefore, securing networks and information systems is essential.

This process referred to as information system network security—focuses on maintaining the availability, confidentiality, and integrity of information assets. These protective measures form the foundation for sustaining business operations and ensuring user trust in organizational technology infrastructures (Amalia & Nasution, 2024; Nasution, 2024; Aji, 2023).

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 1, May 2025
https://doi.org/10.47709/brilliance.v5i1.6162

LITERATURE REVIEW

Computer network security has become a crucial concern in today's increasingly digital environment. According to Stallings (2017), data integrity, confidentiality, and availability are the foundational pillars of information security. One of the most commonly employed tools to support these principles is the firewall. A firewall acts as a barrier between a trusted internal network and potentially harmful external networks by filtering traffic based on predefined rules. Tanenbaum and Wetherall (2011) emphasize that firewalls are essential components in network security architecture due to their ability to block unauthorized access and monitor suspicious activity.

To address various network security requirements, different kinds of firewalls have been designed, such as packet-filtering, stateful inspection, and application-layer firewalls. Each type comes with its own set of strengths and weaknesses concerning efficiency, adaptability, and the degree of protection offered. According to Zwicky et al. (2000), a firewall's success in securing a network heavily relies on how well it is configured and the quality of the security rules applied. Poorly configured firewalls can unintentionally create vulnerabilities that expose systems to cyberattacks. As a result, having technical skills and a strong understanding of the network structure is essential to ensure effective firewall implementation.

While firewalls are an essential element in safeguarding networks, they cannot provide complete protection on their own. Gupta and Sharman (2008) suggest that firewalls should be integrated with additional security measures, including intrusion detection systems (IDS), antivirus programs, and clearly defined security policies. Adopting a multi-layered defense strategy—commonly referred to as "defense in depth"—is viewed as a more effective method for addressing the increasing complexity of cyber threats. Therefore, implementing a firewall should be seen as just one part of a broader, more comprehensive approach to network security in order to ensure robust data protection.

METHOD

Network security is a critical aspect of computer network implementation. Numerous networks have experienced disruptions due to the negligence of network administrators during the design and setup process (Alfredo & Sulistyo, 2023; Arbie & Raharjo, 2024; Sutrisman et al., 2022). This study employs a literature review method to gather relevant data and information from previous research. The literature review serves as a foundation for understanding underlying reasons and supporting references for designing effective network security systems (Satria & Ramadhani, 2023; Wadly, Septian, & Ramadhan, 2023; Subandi, Sugara, & ..., 2023).

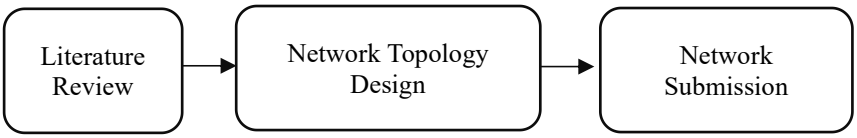

Figure 1 shows the steps in implementing network security using a firewall as a network security strategy

A firewall is a type of network security system designed to regulate data traffic within a computer network (Putra et al., 2023). It functions as a protective barrier, filtering data based on predefined rules to block unauthorized access and defend the network from various external threats such as hackers, viruses, and malware (Jahir & Hamza, 2024; Kurniawan, Purnama, & ..., 2024; Wijayanto et al., 2022; Asian & Erlangga, 2023). One of the key functions of a firewall is to restrict unauthorized access, whether from external sources via the internet or from internal users attempting to reach restricted systems or data (Santoso & Raharjo, 2022; Alhamri, Eliyen, & Heriadi, 2023; Gamaliel & Arliyanto, 2022). As a core component in a layered defense strategy, firewalls play a crucial role in securing network infrastructure. However, to ensure comprehensive protection, firewalls should be used alongside other security measures such as Intrusion Detection and Prevention Systems (ID/IPS), antivirus software, and continuous network monitoring (Santoso & Raharjo, 2022).

Network Topology Design.

Network topology design serves as both a structural concept and a foundation for research implementation. As a conceptual framework, it illustrates how various devices are interconnected and communicate within a network environment. In research contexts, network topology is more than just a technical layout—it acts as the basis for conducting experiments and evaluating specific parameters or variables within the study (Soleman & Soewito, 2024; Amru & Wijaya, 2022).

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, Number 1, May 2025
https://doi.org/10.47709/brilliance.v5i1.6162

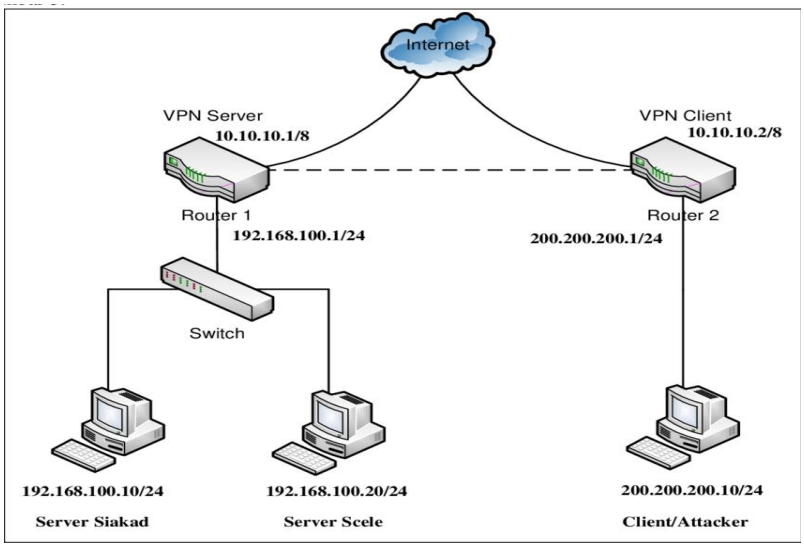

Figure 2. Virtual Private Nerwork Network Topology Design

The network topology illustrated in the diagram represents the implementation of a Virtual Private Network (VPN) (Setyantoro et al., 2022; Faisal, Handoko, & Putra, 2024). This setup demonstrates how two geographically separated local networks can be interconnected. Through VPN technology, these distinct networks can operate as if they are part of the same local environment, enabling secure communication. The VPN ensures both confidentiality and data integrity by utilizing encrypted communication channels (Fajrin, Priatno, & Effendi, 2024; Syahputra, Indriyani, & Sandi, 2023; Awaludin, Yasin, & Risyda, 2024).

Network Testing.

Network testing is a critical phase conducted within a controlled and secured test environment to evaluate connection performance. This phase operates in a closed mode, allowing for the control and restriction of unknown MAC addresses, thereby enhancing network security (Mohamed & Alosman, 2024). To achieve comprehensive system protection, limiting access from unrecognized MAC addresses is essential in preventing unauthorized intrusion (Amru & Wijaya, 2022). Testing is also conducted to validate the effectiveness of configuration setups, particularly before and after the application of knockport technology. Additionally, this process includes port scanning and sniffing to detect any vulnerabilities that may be exploited by potential attackers (Setiawan & Raharjo, 2023; Barra, Sujatmika, & Umami, 2022; Syahputra, Nurcahyo, & Arlis, 2024).

RESULT

This study demonstrates that implementing firewalls as a computer network security strategy significantly enhances data protection against various cyber threats (Wowor, Sudirman, & ..., 2023). Firewalls not only block unauthorized access but also help regulate network traffic by enforcing specific access rules—for instance, permitting only certain IP addresses or applying access restrictions. This is crucial for safeguarding data, especially since many breaches exploit weaknesses in network access control (Azwar & Susantok, 2024; Heremba, Irjanto, & Bun, 2025; Khairunnisa, Annisa, & ..., 2024b). Moreover, firewalls should be integrated with other security measures such as antivirus software, intrusion detection/prevention systems (ID/IPS), and data encryption to create a comprehensive, layered defense. This is essential because firewalls alone are insufficient to counter internal threats or sophisticated attacks like phishing and social engineering (Martanto et al., 2024; Laksana & Mulyani, 2024).

Reduction of Unauthorized Access.

Following the implementation of the firewall, attempts at unauthorized access to the internal network significantly declined. System logs indicated that suspicious data traffic was successfully blocked by the security protocols in place (Khairunnisa, Annisa, & ..., 2024a; Fitrian et al., 2025; Anam & Fachri, 2025). The firewall was specifically configured to reject all unidentified external IP address connections and to restrict traffic on ports that were not in use. These security measures effectively prevented numerous malicious activities from reaching the core system infrastructure (Reyfaldi & Rahmatulloh, 2024; Gunawan, 2025; Shafiyyah, Nama, & ..., 2024).

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 1, May 2025
https://doi.org/10.47709/brilliance.v5i1.6162

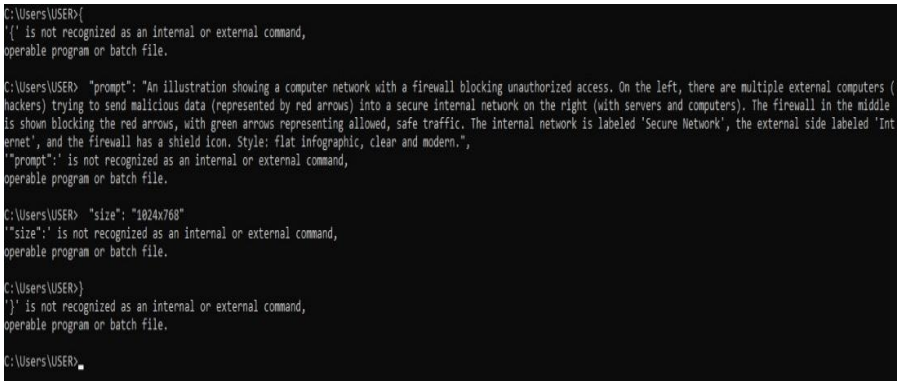

Figure 3. Illustration of Unauthorized Access Blocking by Firewall

The figure above provides a visual representation of how a firewall functions to block unauthorized access to an internal network. It illustrates how malicious traffic or intrusion attempts—such as those from hackers or malware originating outside the network—are effectively filtered and denied (Mauludin & Kuswanto, n.d.).

Improved Network Traffic Control.

Firewalls enable the filtering of data traffic based on designated IP addresses, protocols, and ports. This functionality allows network administrators to implement more precise and restrictive access controls, thereby minimizing potential security vulnerabilities (Widiantara & Kurniawan, 2024; Sulistyo, 2025; Ramadhani, Palasara, & Gani, 2025).

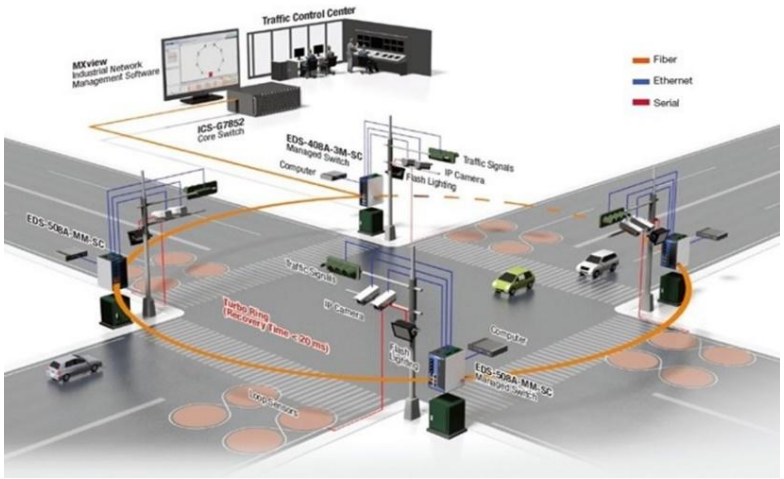

Figure 4. Illustration of Network Traffic Control Improvement.

The figure illustrates how a firewall filters network traffic based on specific parameters. Displayed on the left are key traffic attributes such as IP address, protocol, and port, which are used as the basis for access control and filtering decisions (Syafitri, Lamada, & ..., 2024).

Effectiveness in Malware Prevention.

Integrating a firewall with an intrusion detection system (IDS) and antivirus software is an effective strategy to prevent malware from spreading across a network. Suspicious traffic patterns are detected and blocked at an early stage, stopping them before they reach the core system (Widiantara & Kurniawan, 2024). Although firewalls are not the same as antivirus programs, they serve as the first line of defense in a network security framework. They help prevent malicious traffic—including malware—from entering the network by filtering and blocking unauthorized or harmful connections (Bachtiar, Rahaningsih, & ..., 2024; Sadikin, 2023).

DISCUSSION

While firewall implementation has been shown to significantly enhance network security, relying solely on firewalls does not provide complete protection. To ensure robust security, firewalls must be integrated with complementary systems such as antivirus software, intrusion detection/prevention systems (ID/IPS), and data encryption mechanisms (Fauzan Prasetyo Eka Putra et al., 2024; Eka Putra et al., 2024). This integration is crucial because advanced cyber threats—such as phishing and social engineering—are capable of bypassing conventional

E-ISSN : 2807-9035
Volume 5, Number 1, May 2025
https://doi.org/10.47709/brilliance.v5i1.6162

firewall defenses. As the initial barrier against malicious traffic, firewalls play a vital role in blocking threats before they reach critical systems. However, the effectiveness of a comprehensive network security solution depends on adopting a layered security approach. Combining firewalls with IDS, antivirus tools, and strong security governance is essential to counter the complexities of modern cyberattacks (Haidar et al., 2021).

CONCLUSION

Firewall implementation has proven to be one of the most effective strategies for improving computer network security, especially in the context of data protection. Through testing and observation, firewalls can filter data traffic based on specific rules, prevent unauthorized access, and block suspicious network activities such as port scanning, malware injection, and DOS (DOS) attacks (DOS). In addition, firewalls can also help network administrators monitor, log, and analyze network activities in real time. This is very useful for abatement and forensic processes. However, the effectiveness of firewalls depends heavily on configuration, system updates, and integration into other security technologies. Firewalls are not just one solution, they are part of a layered security approach. Based on the results of the research and analysis conducted, it is recommended that all organizations or institutions that rely on computer networks immediately implement firewalls as a major component of their security system. Firewall configuration should be done by experts regarding potential risks, taking into account the type of service, specific network requirements from the user's perspective. In addition, the development of the entire network security guidelines is an important part that should not be overlooked. Firewalls should not work alone, but they should be integrated into a larger, comprehensive security system. Using network segmentation, role-based access restrictions, and additional technologies such as VPN and data encryption are highly recommended to enhance the protection of sensitive data. Regular cybersecurity training and coaching for all network users should also be kept to generate a comprehensive awareness of digital security.

REFERENCES

Affandi, M. (2022). Implementasi virtual private network (VPN) OpenVPN dengan keamanan sertifikat SSL pada network attached storage (NAS) FreeNAS. *Jurnal Impresi Indonesia, 1*(12), 1329–1341. https://doi.org/10.58344/jii.v1i12.748

Syahab, A. S. (2023). Analisis audit keamanan informasi website menggunakan metode Network Mapper dan Qualys SSL. *Jurnal Manajemen Informatika dan Sistem Informasi, 6*(1), 39–47. https://doi.org/10.36595/misi.v6i1.742

Alfredo, M. J., & Sulistyo, W. (2023). Perancangan sistem keamanan jaringan berbasis hierarchical network design. *IT-Explore: Jurnal Penerapan Teknologi Informasi dan Komunikasi, 2*(1), 48–62. https://doi.org/10.24246/itexplore.v2i1.2023.pp48-62

Arbie, F. R., & Raharjo, M. (2024). Implementasi keamanan jaringan dengan metode security profiles menggunakan Fortigate pada Komisi Aparatur Sipil Negara. *Jurnal Informatika Terpadu, 10*(1), 27–34. https://doi.org/10.54914/jit.v10i1.1060

Ariyadi, T., & Pohan, M. R. (2023). Implementation of penetration testing tools to test Wi-Fi security levels at the Directorate of Innovation and Business Incubators. *Jurnal Penelitian Pendidikan IPA, 9*(12), 10768–10775. https://doi.org/10.29303/jppipa.v9i12.5551

Asian, J., Erlangga, D., & Ayu, M. (2024). Data exfiltration anomaly detection on enterprise networks using deep packet inspection. *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, 22*(3), 665–672. https://doi.org/10.30812/matrik.v22i3.3089

Eka Putra, F. P., Hamzah, A., Agel, W., & Kusuma, R. O. F. (2024a). Impelementasi sistem keamanan jaringan Mikrotik menggunakan firewall filtering dan port knocking. *Jurnal Sistim Informasi dan Teknologi, 5*(4), 82–87. https://doi.org/10.60083/jsisfotek.v5i4.329

Fajrin, B. S., Priatno, P., & Effendi, M. R. (2014). Penerapan sistem keamanan jaringan menggunakan VPN dengan metode PPTP pada PT Hinoka Sinergi Tanyo. *Jurnal Sistem Informasi Universitas Suryadarma, 11*(2). https://doi.org/10.35968/jsi.v11i2.1252

Gamaliel, F., & Arliyanto, P. Y. D. (2023). Perancangan jaringan WiFi dengan menggunakan top down network design. *Jurnal Informatika dan Rekayasa Elektronik, 6*(2), 140–147. https://doi.org/10.36595/jire.v6i2.819

Gunawan, A., Rahmah, R., & Iskandar, A. (2023). Rancang bangun jaringan hotspot menggunakan LINUX ClearOS dengan konsep security gateway. *JTIM: Jurnal Teknologi Informasi dan Multimedia, 4*(4), 272–280. https://doi.org/10.35746/jtim.v4i4.251

Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analisis pengamanan jaringan menggunakan router Mikrotik dari serangan DoS dan pengaruhnya terhadap performansi. *Komputika: Jurnal Sistem Komputer, 11*(1), 67–76. https://doi.org/10.34010/komputika.v11i1.5227

Herdiantoro, H. R., & Islami, M. R. R. (2023). Implementasi two-factor authentication (2FA) dan firewall policies dalam mengamankan website. *Jurnal Mahasiswa Ilmu Komputer, 4*(1), 1–9. https://doi.org/10.24127/ilmukomputer.v4i1.3300

E-ISSN : 2807-9035
Volume 5, **Number** 1, May 2025
https://doi.org/10.47709/brilliance.v5i1.6162

Innuddin, M., Irfan, P., & Hammad, R. (2023). Meningkatkan keamanan web server Nginx dengan NAXSI sebagai web application firewall. *Jurnal Aplikasi Teknologi Informasi dan Manajemen (JATIM), 4*(2), 148–156. https://doi.org/10.31102/jatim.v4i2.2310

Insani, P. P., Kanedi, I., & Akbar, A. A. (2023). Implementation of Snort as a wireless network security detection tool using Linux Ubuntu. *Jurnal Komputer, Informasi dan Teknologi, 3*(2). https://doi.org/10.53697/jkomitek.v3i2.1488

Liu, Y., Tantithamthavorn, C., Li, L., & Liu, Y. (2022). Deep learning for Android malware defenses: A systematic literature review. *ACM Computing Surveys, 55*(8). https://doi.org/10.1145/3544968

Maulana, A., Suharto, N., & Hariyadi, A. (2023). Application of MikroTik firewall for website access restriction and prevention of DoS (Denial of Service) attacks on internet networks Al-Mahrusiyah Vocational School Lirboyo. *Jartel, 13*(1). https://doi.org/10.33795/jartel.v13i1.547

Mendrofa, Y., & Fauzi, R. (2023). Implementasi keamanan jaringan menggunakan port knocking. *Computer and Science Industrial Engineering (COMASIE), 9*(7), 30. https://doi.org/10.33884/comasiejournal.v9i7.7890

Ilham, M., Gunawan, I., & Siregar, Z. A. (2022). Keamanan jaringan WLAN dengan metode firewall filtering menggunakan Mikrotik pada SMP Negeri 1 Dolok Merawan. *Jurnal Ilmiah Sistem Informasi dan Ilmu Komputer, 2*(3), 01–16. https://doi.org/10.55606/juisik.v2i3.309

Mohamed, M., & Alosman, K. (2024). A comprehensive machine learning framework for robust security management in cloud-based Internet of Things systems. *Jurnal Kejuruteraan, 36*(3), 1055–1065. https://doi.org/10.17576/jkukm-2024-36(3)-18

Mohammadzadeh, A., Taghavifar, H., Zhang, Y., & Zhang, W. (2024). A fast nonsingleton Type-3 fuzzy predictive controller for nonholonomic robots under sensor and actuator faults and measurement errors. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 54*(7), 4175–4187. https://doi.org/10.1109/TSMC.2024.3375812

Naufal, F. M., Vahlevi, M. R., Widayana, A., Zulfa, M. L., & Juardi, D. (2022). Implementasi keamanan hotspot menggunakan proxy dan firewall dalam mengatasi resiko ancaman serangan. *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, 8*(2), 148. https://doi.org/10.24014/rmsi.v8i2.17691

Nurdin Prasetiyawan, A., Stiyo Budi, B., Abdillah, M. F., & Riyadi, S. (2024). Sistem keamanan jaringan deteksi dan blok trafic Browsec VPN melalui Mikrotik. *Jurnal Sistem Informasi Aplikasi Teknologi Informasi, 1*(2). https://doi.org/10.53567/josiati.v1i2.17

Peniarsih, P., & Iswandir, I. (2014). Firewall dan iptables pada jaringan komputer. *Jurnal Sistem Informasi Universitas Suryadarma, 11*(2). https://doi.org/10.35968/jsi.v11i2.1241

Permana, H., & Mitro, S. (2024). Proteksi internet di SMKN 3 Pandeglang menggunakan firewall. *Power Elektronik: Jurnal Orang Elektro, 12*(3), 192–195. https://doi.org/10.30591/polektro.v12i3.6073

Putri, H. A., Djibran, N., & Tulloh, R. (2023). Implementation of next-generation firewalls to protect applications from malware attacks. *Jurnal Indonesia Sosial Teknologi, 4*(11), 1961–1970. https://doi.org/10.59141/jist.v4i11.797

Puntadheva, S. A., Kusumaningsih, R. Y. R., & Triyono, J. (2023). Perancangan keamanan jaringan komputer menggunakan firewall intrusion detection system (IDS) terhadap serangan brute force dan implementasi ARP list. *Jurnal Jarkom, 10*(2), 32–37. https://doi.org/10.34151/jarkom.v10i2.4482

Sari, Y. N., Irfan, D., & Huda, A. (2022). Network security analysis using virtual private network in vocational school. *Jurnal Paedagogy, 9*(3), 582. https://doi.org/10.33394/jp.v9i3.5346

Satria, A., & Ramadhani, F. (2023). Analisis keamanan jaringan komputer dengan menggunakan switch port security di Cisco Packet Tracer. *Sudo Jurnal Teknik Informatika, 2*(2), 52–60. https://doi.org/10.56211/sudo.v2i2.260

Styorini, W., Azwar, H., & Susantok, M. (2024). Implementasi firewall pada laboratorium jaringan komputer SMAIT AL-ITTIHAD. *JITER-PM (Jurnal Inovasi Terapan - Pengabdian Masyarakat), 2*(1), 38–44. https://doi.org/10.35143/jiter-pm.v2i1.6162

Subakti, A. J. (2023). Analysis of Lapan security access based on firewall log in Center Eight. *Jurnal Manajemen Informatika Medicom (JMI), 11*(1), 26–31. https://doi.org/10.35335/jmi.v11i1.52

Syafi'i Bachtiar, M., Rahaningsih, N., & Danar Dana, R. (2024). Firewall filtering berbasis deep packet inspection dalam mendeteksi dan mencegah ancaman malware. *JATI (Jurnal Mahasiswa Teknik Informatika), 8*(1), 399–405. https://doi.org/10.36040/jati.v8i1.8387

Syamsu, M., & Widodo, W. (2022). Implementasi arsitektur firewall sebagai sistem keamanan jaringan WiFi 802.11ax Aruba Software Defined WAN (SD-WAN). *Jurnal Teknologi Informasi (JUTECH), 3*(2), 141–157. https://doi.org/10.32546/jutech.v3i2.2033

Syaputera, A., Riska, R., & Mardiana, Y. (2023). Hotspot network security system from brute force attack using pfSense external firewall (Case study of Wifi-Ku.Net Hotspot). *Jurnal Komputer, Informasi dan Teknologi, 3*(1). https://doi.org/10.53697/jkomitek.v3i1.1286

Wadly, F., Septian, R., & Ramadhan, Z. (2023). Strategi penanggulangan kelemahan terhadap ancaman keamanan pada jaringan wireless. *Jurnal Nasional Teknologi Komputer, 3*(2), 59–67. https://doi.org/10.61306/jnastek.v3i2.89

Wang, S., Xu, W., & Liu, Y. (2023). Res-TranBiLSTM: An intelligent approach for intrusion detection in the Internet of Things. *Computer Networks, 235*, 109982. https://doi.org/10.1016/j.comnet.2023.109982

E-ISSN : 2807-9035
Volume 5, **Number** 1, May 2025
https://doi.org/10.47709/brilliance.v5i1.6162

Wang, X., Wu, Z., Jia, M., Xu, T., Pan, C., Qi, X., & Zhao, M. (2023). Lightweight SM-YOLOv5 tomato fruit detection algorithm for plant factory. *Sensors, 23*(6), Article 3336. https://doi.org/10.3390/s23063336

Wowor, H. G. A., Sudirman, A., & Hakiki, F. (2024). China's Great Firewall: Cybersecurity as strategy for building world cyberpower. *JISPO: Jurnal Ilmu Sosial dan Ilmu Politik, 13*(2), 193–232. https://doi.org/10.15575/jispo.v13i2.27713

Yuliandari, D., Walim, W., Raja, B. K., Ningsih, R., & Wahidin, A. J. (2023). Simulasi penerapan sistem monitoring jaringan Snort NIDS pada web server menggunakan metode SPDLC. *Jurnal Infortech, 5*(2), 133–138. https://doi.org/10.31294/infortech.v5i2.17338

Yusril Amru, & Ermadi Satriya Wijaya. (2022). Analisis penerapan Sangfor NGAF firewall sebagai keamanan pada jaringan internet Universitas Muhammadiyah Purwokerto. *Jurnal Sistem Informasi (JUSIN), 3*(2), 55–66. https://doi.org/10.32546/jusin.v3i2.1959

Zhou, L., Leng, S., Wang, Q., & Liu, Q. (2023). Integrated sensing and communication in UAV swarms for cooperative multiple targets tracking. *IEEE Transactions on Mobile Computing, 22*(11), 6526–6542. https://doi.org/10.1109/TMC.2022.3193499

Zulmy Alhamri, R., Eliyen, K., & Heriadi, A. (2023). Pengembangan aplikasi remote berbasis Android untuk konfigurasi intrusion prevention system memanfaatkan Internet of Things. *Jurnal Mnemonic, 6*(2), 135–148. https://doi.org/10.36040/mnemonic.v6i2.6727

Zy, A. T., Isarianto, Rifai, A. M., Nugroho, A., & Ghofir, A. (2025). Enhancing network security: Evaluating SDN-enabled firewall solutions and clustering analysis using K-means through data-driven insights. *Jurnal RESTI, 9*(1), 69–76. https://doi.org/10.29207/resti.v9i1.6056