

Pemanfaatan Mikrotik Rb941-2nd menggunakan metode *firewall filtering* untuk keamanan jaringan dengan model forensik pada kantor desa

Rahmat Sulaiman^{1*}, Padli¹, Agustina Mardeka Raya²

¹Program Studi Teknik Informatika

Fakultas Teknologi Informasi, Institut Sains dan Bisnis Atma Luhur

Jl. Jend. Sudirman, Pangkalpinang, Kepulauan Bangka Belitung, Indonesia. 33117

*E-mail: rahmatsulaiman@atmaluhur.com

²Program Studi Sistem Infromasi

Fakultas Teknologi Informasi, Institut Sains dan Bisnis Atma Luhur

Jl. Jend. Sudirman, Pangkalpinang, Kepulauan Bangka Belitung, Indonesia. 33117

Abstrak: Seiring dengan meningkatnya permintaan akan layanan yang cepat dan efektif, perkembangan teknologi dan telekomunikasi global juga meningkat. Setiap kantor desa salah satunya Belo Laut harus memiliki jaringan internet untuk melayani masyarakat dalam mengakses data masyarakat. Oleh karena itu perkembangan teknologi dan telekomunikasi juga sangat penting bagi pemerintah. Untuk menciptakan jaringan internet yang aman dan efektif, sistem keamanan jaringan ini menggunakan Mikrotik dengan metode *Firewall Filtering*. Masalah penelitian adalah merancang dan membangun keamanan jaringan di area kantor desa Belo Laut menggunakan Mikrotik untuk mencegah dampak negatif dari internet, seperti situs yang berbau konten dewasa. Konfigurasi layer 7 protokol dan *filter rules* termasuk dalam pemblokiran. Berdasarkan kata kunci yang telah ditentukan, hasil pengujian menunjukkan bahwa Mikrotik berhasil memblokir situs atau *website* yang berbau konten dewasa.

Kata Kunci: *filter rules*, firewall filtering, forensik, keamanan jaringan, Mikrotik

Abstract: Nowadays as demand for fast and effective services increases, global technological and telecommunications developments also increase. Every village office, one of which is Belo Laut, must have an internet network to serve the community in accessing community data. Therefore the development of technology and telecommunications is also very important for the government. To create a safe and effective internet network, this network security system uses Mikrotik with the firewall filtering method. The research problem is how to design and build network security in the Belo Laut village office area using Mikrotik to prevent the negative impacts of the internet, such as sites with adult content. Layer 7 protocol configuration and filter rules are included in blocking. Based on the keywords that have been determined, the test results show that Mikrotik has succeeded in blocking sites or websites that contain adult content.

Keywords: filter rules, firewall filtering, forensic, network security, mikrotik

PENDAHULUAN

Teknologi saat ini telah mencakup seluruh aspek kehidupan dan juga telah berkembang ke seluruh dunia. Karena itu faktanya bahwa internet adalah satu-satunya komputer jaringan terbuka di dunia, tidak ada jaminan keamanan untuk jaringan yang terhubung ke internet. Hal ini mengindikasikan bahwa jaringan yang terkoneksi internet kemungkinan besar akan mudah diakses oleh individu yang belum diundang dari luar jika operator jaringan kurang hati-hati dalam mengelola sistem. Peretas dapat dengan mudah memasuki jaringan dan menyebabkan gangguan dengan

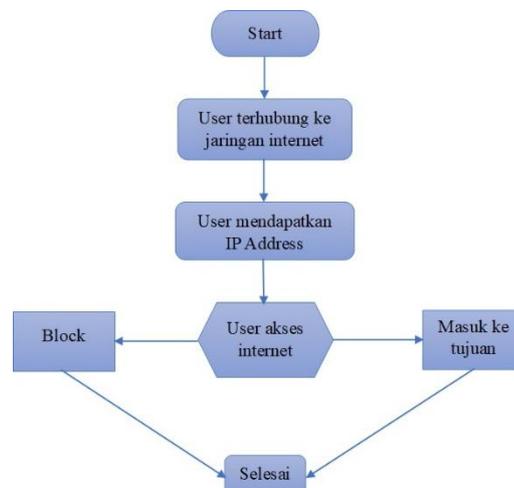
memanfaatkan celah dan *port* yang terbuka. Konsekuensinya, diperlukan *firewall* atau sistem keamanan jaringan untuk mengatasi hal tersebut (Barra et al., 2022).

Dengan jaringan internet pula dimungkinkan untuk menghubungkan orang-orang melintasi jarak ratusan atau bahkan jutaan kilometer menggunakan jaringan Internet. Karena tidak pernah ada koneksi antara internet dan jaringan komputer, kedua jaringan tersebut sangat terkait Pengiriman data dari satu komputer ke komputer lainnya dapat dipercepat dengan adanya jaringan internet. Faktanya, kedua jaringan ini sekarang menjadi blok bangunan dasar pekerjaan, tidak sedikit perusahaan yang mengandalkan kedua perusahaan ini untuk siklus, barang, dan segala sesuatu yang berhubungan dengan bisnis mereka. Alhasil, berbagai pihak memantau dan mengikuti perkembangan setiap perkembangan jaringan internet dan komputer (Ilham et al., 2022). *Router* Mikrotik adalah alat atau perangkat yang dapat menghubungkan organisasi dengan organisasi yang berbeda. Sekilas *router* dan *bridge* mirip namun *bridge* tidak memiliki kecerdasan *router*. Sakelar berfungsi menggunakan tabel kemudi yang disimpan dalam memori untuk menentukan pilihan dimana dan bagaimana paket dikirim. Paket data yang berjalan pada rute terbaik dapat dihindari oleh *router* (Ilham et al., 2022).

Berdasarkan pemaparan latar belakang, sehingga sangat diperlukan pemanfaatan Mikrotik yang bertujuan untuk mempermudah staf dan pegawai akan lebih mudah dan lebih aman dalam mengakses data-data dan informasi saat sedang berkerja, dan mengetahui kerentanan keamanan informasi akibat serangan DoS dan DDoS pada kantor desa Belo Laut.

METODE PENELITIAN

Penelitian ini dilaksanakan pada tahun 2023 hingga 2024 awal. Penelitian ini mengkaji perilaku staf dan karyawan serta memberikan solusi terhadap permasalahan yang mereka temui di ruang lingkup kantor desa. Penelitian ini meneapkan metode *firewall filtering* yangmana merupakan jenis *firewall* yang paling mendasar yang tugasnya memeriksa paket hanya dari perspektif luar, misalnya, lokasi IP sumber dan tujuan, konvensi, dan nomor *port*. *Firewall* semacam ini tidak akan membuka item dalam parsel dengan benar-benar melihat keamanan paket. Dengan cara ini, jika dari pemeriksaan luar paket tersebut dianggap berisiko, paket tersebut akan secara alami diberhentikan, *firewall filtering* juga digunakan untuk menyaring atau membatasi akses atau *searching* dari karyawan Desa Belo Laut Bangka Barat.



Gambar 1. Metode *firewall filtering*

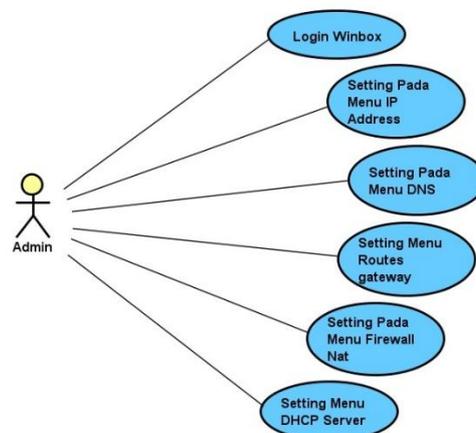
Selain menerapkan metode *firewall filtering* penelitian ini juga memanfaatkan metode forensik. Forensik adalah studi tentang fakta dan kemampuan untuk mengumpulkan data dari lingkungan sekitarnya. Jaringan forensik adalah cabang forensik digital di mana bukti diperoleh dari jaringan dan ditafsirkan menggunakan pengetahuan jaringan yang beragam. Fungsi model forensik di sini yaitu adalah untuk menjelaskan secara menyeluruh mengenai tahap-tahap dan proses yang dilakukan penulis dalam penelitian, model *forensik* juga di gunakan untuk melihat apakah ada serangan yang terjadi terhadap sistem yang sudah di buat melalui aplikasi *winbox*.

HASIL DAN PEMBAHASAN

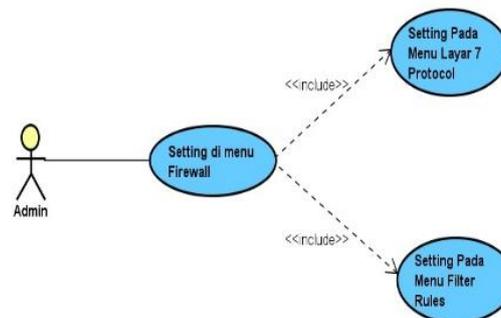
Kantor Desa Belo Laut adalah kantor desa yang bergerak di bidang *government/* pemerintah. Kantor Desa Belo Laut bertugas mengatur dan mengurus perkembangan desa, mereka juga melayani masyarakat dan kemajuan Desa Belo Laut. Kantor Desa Belo Laut menggunakan internet tipe ISP *Icon+*. Masalah yang dihadapi adalah salah satu laptop/PC karyawan Desa Belo Laut sering terkena virus ketika sedang membuka situs-situs ilegal, belum adanya perlindungan pada jaringan internet di kantor Belo Laut seperti penerapan konfigurasi *firewall* lainnya, karena belum adanya perlindungan pada jaringan kantor desa Belo Laut membuat kepala desa atau karyawan khawatir akan serangan-serangan yang bisa membahayakan jaringan dan data yang ada di kantor Desa Belo Laut.

1. Use case diagram sistem

Use Case diagram di bawah menjelaskan gambaran intraksi dan fungsional antara admin dan *Winbox*, penulis juga membuat deskripsi yang bertujuan untuk menjelaskan setiap fungsi dari komponen *use case* tersebut.



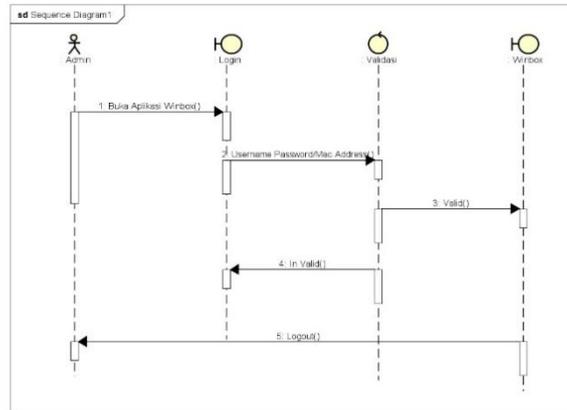
Gambar 2. Use case diagram sistem usulan admin konfigurasi *ethernet*



Gambar 3. Use case diagram sistem usulan admin *block* situs

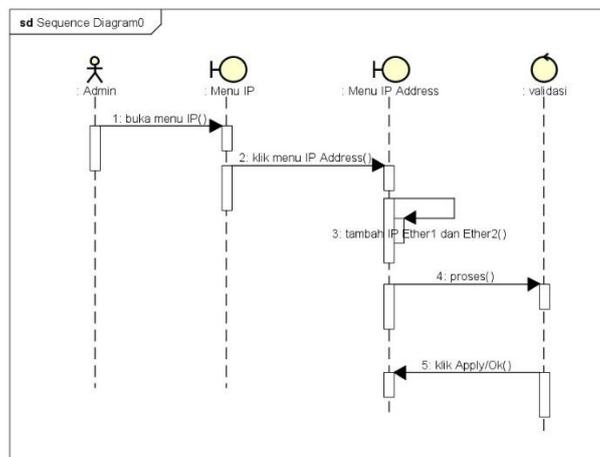
2. Sequence diagram sistem usulan

Di bawah ini merupakan *sequence* diagram sistem usulan admin dalam melakukan login aplikasi *Winbox*, koneksi Mikrotik ke jaringan *Ethernet*, dan admin *block* situs menggunakan *Firewall*.



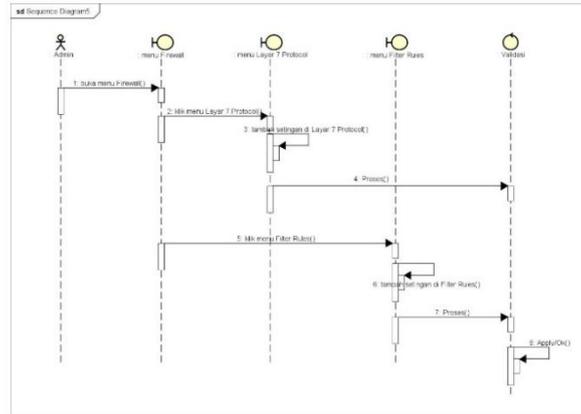
Gambar 4. Sequence diagram sistem usulan login Winbox

Berdasarkan Gambar 4, *sequence* diagram sistem usulan login Winbox menjelaskan proses atau langkah-langkah admin dalam melakukan login ke Winbox. Pertama yang dilakukan oleh admin adalah membuka aplikasi Winbox, kemudian admin masuk menggunakan username/password jika sudah diatur (*setting*), jika belum admin bisa masuk melalui *Mac.Address* yang tampil di menu *neighbors*.



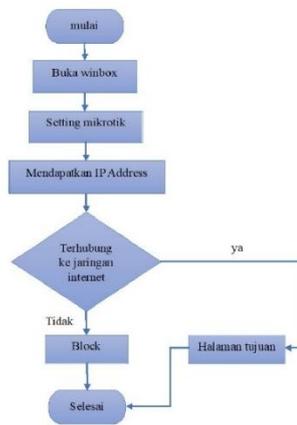
Gambar 5 Sequence diagram admin setting IP address

Sequence diagram sistem usulan *setting* IP address pada Gambar 5 menjelaskan proses atau langkah admin dalam *setting* IP address. Pertama yang dilakukan admin adalah buka menu IP, kemudian admin klik menu IP Address pada Winbox, lalu klik tanda tambah untuk menambahkan IP *Ether1* 192.168.1.5/24 dan *Ether2* 192.168.50.1/24 setelah selesai klik *Apply* lalu *Ok*. Pada Gambar 6 *sequence* sistem usulan admin *block* situs melalui *firewall* menjelaskan tahap-tahap admin dalam melakukan pemblokiran yaitu yang pertama admin buka menu *firewall*, setelah itu klik menu *Layar 7 Protocol* kemudian tambah *settingan* di *layar 7* protokol mengenai situs apa yang ingin diblokir kemudian klik *Apply/OK*, kemudian klik menu *filter rules*, tambah *settingan* pada *filter rules* setelah selesai klik *Apply/OK*.



Gambar 6. Sequence admin block situs melalui firewall

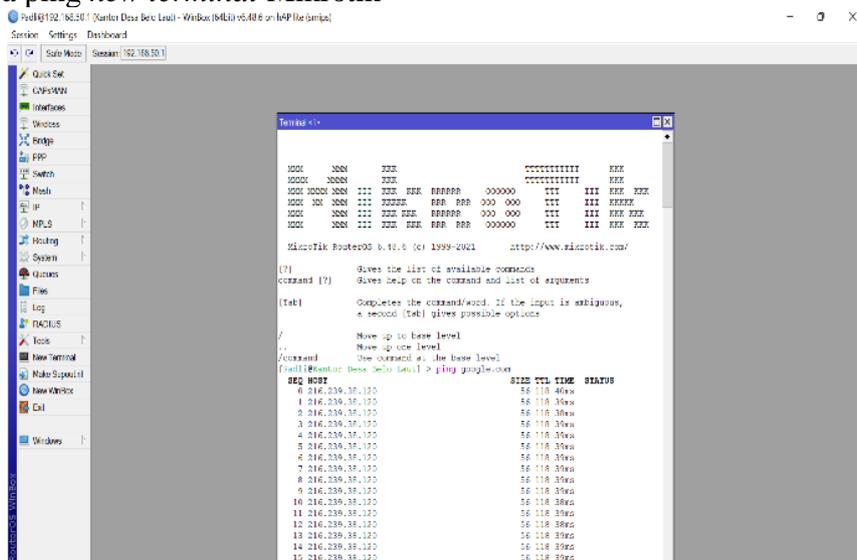
3. Flowchart



Gambar 7. Flowchart

Pada Gambar 7 yaitu yang merupakan penjelasan mengenai tahap-tahap atau proses yang dilakukan penulis dalam penelitian yang sedang dilakukan yang bertempat di kantor Desa Belo Laut.

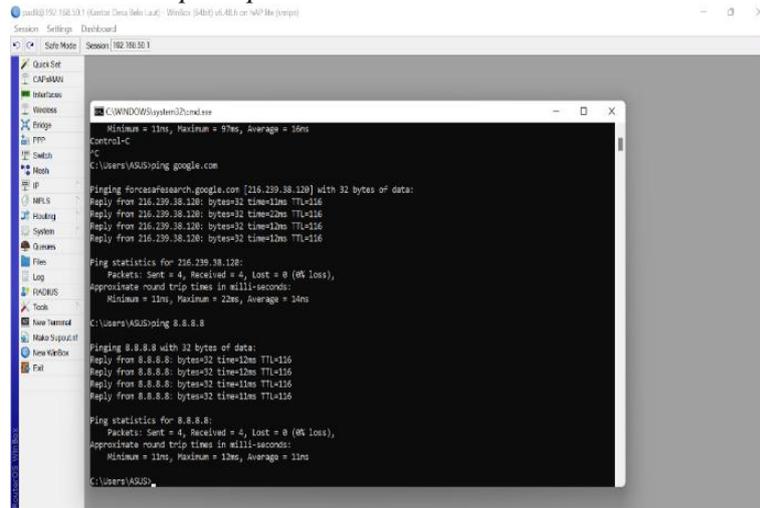
4. Uji coba ping new terminal Mikrotik



Gambar 8. Uji coba ping melalui new terminal

Pada Gambar 8 pengujian melalui *New Terminal* menjelaskan proses admin sedang melakukan tes melalui menu *New Terminal* yang ada di *winbox*, cara untuk mengecek apakah Mikrotik sudah terkoneksi ke jaringan internet apa belum maka admin harus melakukan test ping *google.com* jika tampilan *New Terminal* seperti ditampilkan pada Gambar 8 maka *router* Mikrotik sudah terhubung ke jaringan internet tetapi jika ada tulisan *timeout* dalam pengetesan maka ada kesalahan dalam sistem maka harus diperbaiki sampai tulisan *timeout* hilang.

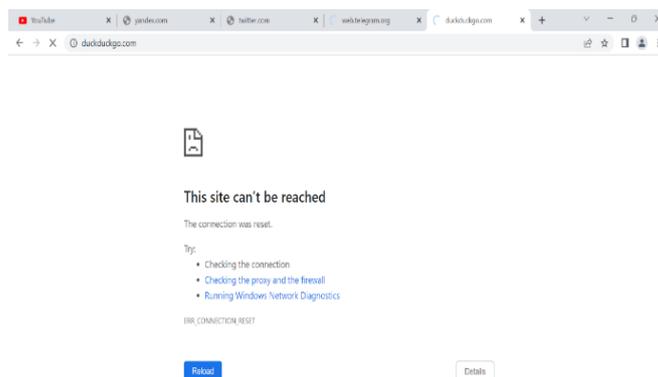
5. Uji coba pada *command prompt*



Gambar 9. Uji coba pada *command prompt*

Pada Gambar 9 merupakan proses admin melakukan uji coba melalui menu *command prompt* untuk memeriksa apakah laptop admin sudah terhubung ke jaringan internet atau belum, jika *ether 2* pada laptop sudah terkoneksi ke jaringan maka hasil tes menampilkan *reply from* tetapi jika salah sistem *command prompt* akan *invalid* dan harus diperbaiki.

6. Uji coba *block situs*



Gambar 10. Uji coba *block situs*

Pada Gambar 9, tahap ini penulis melakukan uji coba memblokir sebuah situs yang berbau dewasa/negatif secara langsung di kantor Desa Belo Laut, pemblokiran

menggunakan aplikasi *Winbox* dengan metode *firewall filtering*, konfigurasi pada menu *Layar 7 Protocol, filter rules* dan menggunakan satu jaringan ya sama, situs yang diblokir di antaranya *Yandex.com, twitter.com, web.telegram.org, duckduckgo.com* Setelah berhasil melakukan pemblokiran bisa dilihat atau dicek di Google Chrome apakah situs berhasil diblokir atau tidak.

KESIMPULAN

Berdasarkan penelitian yang dilakukan dengan metode *firewall filtering* untuk keamanan jaringan pada kantor Desa Belo Laut Bangka Barat, kesimpulan pada penelitian ini yaitu tujuan dari keamanan jaringan menggunakan Mikrotik dengan metode *firewall filtering* adalah untuk memudahkan admin di kantor Desa Belo Laut dalam mengamankan jaringan Mikrotik dari serangan luar yang tidak bertanggung jawab. Sistem keamanan jaringan dibuat menggunakan Mikrotik RB941-2ND metode *firewall filtering* dengan model *forensik*, yang bertempat di kantor Desa Belo Laut Bangka Barat. Melakukan *block* pada *website* atau situs yang berbau pornografi, sedangkan *website* atau situs yang tidak berbau pornografi tidak akan diblokir dan akan berhasil masuk ke *website* atau situs yang dituju.

DAFTAR PUSTAKA

- Astari, A. A. (2018). Implementasi keamanan jaringan dengan metode *firewall filtering* menggunakan Mikrotik. *Simki-Techsain*, 2(1).
- Barra, A. R., Sujatmika, R., & Umami, I. (2022). Sistem keamanan jaringan komputer bridge firewall menggunakan router board Mikrotik Rb750. *J. Teknol. Dan Sist. Inf. Bisnis-JTEKSIS*, 4(1), 427-431. <https://doi.org/10.47233/jteksis.v4i2.561>.
- Fasehan, B. (2020). Rancang bangun sistem keamanan jaringan komputer. *Tugas Akhir*. Palembang: Politeknik Negeri Sriwijaya Palembang.
- Gustiawan, M., Yudianto, R. J., Pratama, J., & Fauzi, A. (2021). Implementasi jaringan hotspot di perkantoran guna meningkatkan keamanan jaringan komputer. *J. Nas. Komputasi dan Teknol. Inf.*, 4(4), 244–247. <https://doi.org/10.32672/jnkti.v4i4.3098>.
- Ilham, M., Gunawan, I., Siregar, Z. A. (2022). Keamanan jaringan WLAN dengan metode firewall filtering menggunakan Mikrotik pada SMP Negeri 1 Dolok Merawan. *J. Ilm. Sist. Inf. dan Ilmu Komput.*, 2(3), 1-16. <https://doi.org/10.55606/juisik.v2i3.309>.
- Jayanto, S., Tanton, A., Asyari, H. (2021). Implementasi keamanan jaringan dengan packet filtering berbasis Mikrotik untuk internet positif di SMKN 1 Praya,” *J. Ranah Publik Indones. Kontemporer*, 1(2), 65–77. <https://doi.org/10.47134/rapik.v1i2.10>.
- Lestari, M. A., Tabrani, M., & Ayumida, S. (2021). Sistem informasi pengolahan data administrasi kependudukan pada kantor Desa Pucung Karawang. *J. Interkom J. Publ. Ilm. Bid. Teknol. Inf. dan Komun.*, 13(3), 14–21. <https://doi.org/10.35969/interkom.v13i3.50>.
- Nitra, R. O., & Ryansyah, M. (2019). Implementasi sistem keamanan jaringan menggunakan firewall security port pada vitaa multi oxygen,” *J. Sist. dan Teknol. Inf.*, 7(1), 52-59. <https://doi.org/10.26418/justin.v7i1.29979>.
- Novianto, M. A., & Munir, S. (2022). Analisis dan implementasi restful API guna pengembangan sistem informasi akademik pada perguruan tinggi. *Jurnal Informatika Terpadu*, 8(1), 47–61. <https://doi.org/10.54914/jit.v8i1>.
- Putra, B. J. G., Musri, T., & Gultom, L. M. (2020). Pemanfaatan Mikrotik routerboard sebagai keamanan jaringan dari UDP Flood dengan menggunakan firewall di Dinas Pendidikan Bengkalis,” *Semin. Nas. Ind. dan Teknol. (SNIT)*, 260–269.
- Putra, S. O., & Ramdhani, Y. (2021). Memanfaatkan fitur firewall rules pada Mikrotik untuk keamanan jaringan di Hotel Lenora Bandung. *eProsiding Tek. Inform.*, 2(1), 122–126.
- Riyandari, L., & Purnomo, J. (2020). Rancang bangun jaringan internet dengan memperhatikan etika profesi TI menggunakan web filtering pada router Mikrotik 951G-2HND. *Tek. Teknol. Informasi, Ilmu Komput. dan Manaj.*, 4(1), 35–45.
- Sudaryanto, D. H. (2017). Merancang pengaman (*security*) jaringan komputer. *Swara Patra*, 7(1), 64-73.
- Sudiatmika, I. P. G. A., Ariwanta, I. P. Y. A., & Melati, I. G. A. S. (2022). Mengoptimalkan keamanan

- jaringan komputer menggunakan snort dan telegram bot yang terintegrasi dengan mikrotik,” *J. Comput. Syst. Informatics*, 3(4), 247–256. <https://doi.org/10.47065/josyc.v3i4.2037>.
- Syarif, M., & Nugraha, W. (2020). Pemodelan diagram UML sistem pembayaran tunai pada transaksi e-commerce. *J. Tek. Inform. Kaputama*, 4(1), 64-70.
- Wibowo, A., Hidayat, A. S., & Rahmawati, E. (2020). Pembangunan aplikasi e-commerce pemasaran batik pada Toko Batik Rifqi. *J. Comput. Syst. Informatics*, 1(2), 46–53.
- Widharma, I. G. S. (2020). Pengamanan sistem jaringan komputer dengan teknologi firewall. In *Arsitektur Komputer*, 1-28.
- Yohanness, F. (2020). Analisa dan perancangan keamanan jaringan lokal menggunakan security onion dan mikrotik, *J. Inf. Syst. Technol.*, 1(2), 37–61.