Jurnal Sistim Informasi dan Teknologi

https://jsisfotek.org/index.php

2023 Vol. 5 No. 4 Hal: 82-87 e-ISSN: 2686-3154

Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking

Fauzan Prasetyo Eka Putra[1✉], Amir Hamzah[2], Walid Agel[3], R. Okky Firmansyah Kusuma[4]

[1,2,3,4]Universitas Madura

prasetyo@unira.ac.id

Abstrak

Keamanan jaringan Mikrotik menjadi hal yang penting untuk dipertimbangkan, mengingat semakin maraknya serangan siber yang terjadi. Salah satu cara untuk mengingkatkan keamanan jaringan Mikrotik adalah dengan menerapkan Firewall Filtering dan Port Knocking. Firewall Filtering digunakan untuk memblokir port-port yang rentan terhadap serangan, sedangkan port knocking digunakan untuk menambahkan lapisan keamanan tambahan dengan mengharuskan pengguna untuk memasukkan kombinasi port sebelum dapat mengakses jaringan. Penelitian ini bertujuan untuk mengetahui cara implementasi dari sistem keamanan jaringan Mikrotik menggunakan firewall filtering dan port knocking. Penelitian ini dilakukan dengan menggunakan metode deskriptif. Hasil penelitian menunjukkan bahwa penerapan firewall filtering dan port knocking dapat meningkatkan sistem keamanan jaringan Mikrotik. Firewall filtering dapat memblokir serangan dari luar jaringan, sedangkan port knocking dapat mencegah serangan dari luar jaringan.

Kata kunci: Keamanan Jaringan, Mikrotik, Firewall Filtering, Port Knocking.

1. Pendahuluan

Pada era digital saat ini, infrastruktur jaringan komputer beberapa instansi telah diperbarui dan dilengkapi dengan berbagai peralatan elektronik canggih untuk membantu aktifitas sehari-hari [1]. Di masa-masa yang lalu, disetiap kepentingan yang ada kaitannya dengan militer, jaringan ini sering digunakan [2]. Setiap generasi baru telah menghasilkan transformasi besar dalam cara kita berinteraksi dan berkomunikasi dengan dunia digital, saat ini jaringan adalah salah satu komponen penting dalam kehidupan umat manusia [3][4]. Peningkatan yang terjadi pada bidang ini semangkin melonjak tinggi sehingga peningkatan pertukaran data dan informasi dalam skala dunia pun turut naik [5]. Kemajuan ini meningkatkan konektivitas, latensi rendah, kecepatan, dan kapasitas [6]. Dengan berkembangnya teknologi tersebut tentu juga tidak dapat dipungkiri bahwa dampak positif dari peningkatan tersebut juga dapat menimbulkan potensi yang akan berdampak pada meningkatnya kejahatan siber [7]. Jaringan adalah koneksi dari berbagai perangkat yang dapat melakukan kontak satu sama lain [8]. Jumlah serangan-serangan di internet telah meningkat dalam beberapa tahun terakhir [9]. Oleh karena itu, setiap ahli yang mengatur di bagian *computer network* harus waspada untuk menghadapi meluapnya serangan yang dapat terjadi oleh para pencuri di dunia maya. Serangan DoS merupakan satu dari beberapa jenis serangan yang paling rentan terjadi pada *computer network* dan dilakukan dengan mencegah atau menghalangi seseorang agar mereka tidak dapat dengan mudah menghabiskan sumber daya seperti *bandwith*, memori, CPU, dan ruang disk melalui jaringan, sistem, ataupun aplikasi [7].

Untuk membuat interaksi pengguna lebih nyaman, desain jaringan harus dibuat dengan sesuai agar gampang untuk digunakan dan juga kualitas dari keamanan suatu jaringan yang tidak mudah untuk dibobol, sehingga *computer network* dapat diatur dengan baik [10]. Hal tersebut termasuk menggunakan perangkat lunak terbaru, menggunakan kata sandi yang kuat, dan menghindari terhubung ke jaringan yang tidak aman [11]. Cara untuk mempertahankan suatu jaringan dari beragam jenis yang membahayakan dari luar yang berpotensi untuk mengacaukan jaringan dan mencuri informasi yang ada di perusahaan [12].

Firewall adalah perangkat, baik lunak maupun keras, yang digunakan untuk menerapkan kebijakan keamanan di dalam atau di seluruh jaringan. Perangkat ini berfungsi sebagai penjaga keamanan gateway jaringan, memeriksa paket yang masuk dan keluar dan memperlakukannya sesuai dengan berbagai aturan penyaringan. Dengan demikian, *firewall* memiliki kemampuan untuk memblokir, mengizinkan, atau menjatuhkan lalu lintas [13].

Saat ini, biaya tinggi masih menghalangi pembelian *firewall* yang tangguh. Perangkat *firewall* yang canggih itu hanya dapat diakses oleh instansi besar dan perusahaan kecil. Oleh karena itu, perangkat *firewall* atau keamanan murah diperlukan untuk melindungi jaringan komputer bisnis dan organisasi menengah dan kecil [14]. *Router* Mikrotik adalah sistem operasi dengan banyak fitur yang cukup untuk jaringan nirkabel [15]. Banyak *provider*, seperti ISP, *hotspot*, dan warmet, telah menggunakan Mikrotik sebagai salah satu alternatif yang ada di bidang

Diterima: 02-01-2024 | Revisi: 03-01-2024 | Diterbitkan: 11-01-2023 | doi: 10.60083/jsisfotek.v5i4.329

teknologi. Mikrotik menjadi pilihan umum dalam dunia teknologi informasi dikarenakan telah ditunjuk menjadi jaringan router komputer yang dapat diandalkan. Selain memiliki banyak fitur dan alat yang luar biasa, mikrotik sangat cocok untuk perangkat jaringan, baik kabel maupun nirkabel. Sifat open source mikrotik membuatnya menjadi *router* yang sangat disukai di dunia teknologi informasi. Pentingnya *router* dikarenakan memiliki fungsi untuk mengelola koneksi antara beberapa komputer. pengoperasiannya mudah dan tidak membutuhkan banyak *hardware* [16].
Poin terpenting dalam layanan jaringan adalah keamanan akses port. *Port knocking* merupakan metode yang berfungsi untuk memblokir akses yang tidak diinginkan. Dengan kata lain, jika seseorang perlu mengakses server, mereka harus melakukan ketukan untuk melakukannya, dan port tersebut akan ditutup kembali setelah pengguna selesai menggunakannya [17]. Untuk alasan ini, diperlukan metode keamanan jaringan yang dapat mencegah ancaman serangan seperti itu dan meminimalkan jumlah ancaman serangan yang dapat masuk ke sistem jaringan [18]. Dalam penelitian ini implementasi teknik *firewall filtering* dan *port knocking* untuk menjaga sistem keamanan dari sistem keamanan jaringan *mikrotik*.

2. Metode Penelitian

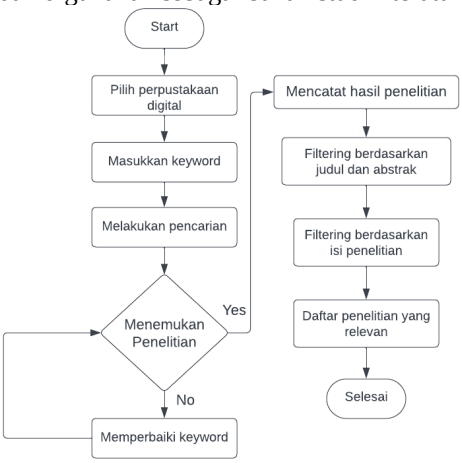
Dua poin penting berikut merupakan metode penelitian yang digunakan pada penelitian ini:

Literature Review

Pada bagian ini kami melakukan analisa pada beberapa artikel dan jurnal yang relevan dengan fokus sistem keamanan pada jaringan *mikrotik* dengan mengaplikasikan *firewall filtering* dan *port knocking* untuk menciptakan sistem jaringan yang dapat diandalkan. Kami melakukan fokus analisis pada artikel yang relevan yang diterbitkan selama 5 tahun terakhir [14].

Seleksi Studi

Jumlah teks yang ditemukan selama pencarian kata kunci awal dan berdasarkan tahun publikasi 2018–2023, berjumlah 50 judul literatur. Sebagian besar dari literatur ini akan ditinjau dan dipilih sesuai dengan kriteria inklusi dan eksklusi. Selama proses seleksi dengan kriteria inklusi, 41 judul literatur yang diperoleh dipisahkan untuk dianalisis kembali sesuai dengan kriteria eksklusi, subjek, dan kemungkinan judul yang terkait. Hasil dari analisis ini menunjukkan bahwa jumlah literatur yang diperoleh secara keseluruhan Selama tahap ini, 30 literatur terkumpul dikumpulkan, dinilai dengan baik, dan digunakan sebagai bahan studi literatur [19].



Gambar 1. Flowchart seleksi studi

3. Hasil dan Pembahasan

Cara Kerja Firewall Filtering

Firewall biasanya digunakan pada *computer network*, lebih spesifiknya pada bagian gateway [20]. *Firewall* akan menggunakan *filter rules* [21]. *Firewall* ini merupakan metode yang dapat memilih keputusan dengan menentukan pemberian atau penolakan akses. Di dalam paket terdapat tipe informasi, alamat asal dan tujuan, kemudian port yang akan digunakan, beberapa hal tersebut dapat dikontrol menggunakan metode *firewall*. Kendati akan hal itu, IP *firewall* tidak dapat sepenuhnya dikatakan aman karena pada bagian tersebut mempunyai *chance* untuk tidak menghiraukan beberapa log yang bisa jadi sangat berguna [22].
Filter jaringan memiliki lima rantai utama yang bisa digunakan, lima rantai tersebut ialah *prerouting, postrouting, input, forward,* dan *output. Prerouting* merupakan langkah awal yang akan dilalui oleh tiap paket yang masuk ke *iptables*. Sebelum masuk pada keputusan *routing,* tiap paket akan mendapati transfigurasi secara signifikan. Hal

itu akan dilanjutkan ke rantai maju jika hal tersebut jika itu diarahkan untuk host yang lain,namun itu akan diarahkan ke host itu sendiri jika hal tersebut dilanjutkan ke rantai *input*. Paket akan diarahkan ke rantai *output* jika terdapat paket yang keluar, namun sebaliknya paket akan masuk ke rantai *input* jika terdapat paket yang masuk, kedua hal tersebut akan ditangani oleh host lokal. Sebelum paket meninggalkan host, paket-paket yang berasal dari *output* dan *forward* terlebih dahulu akan masuk melalui rantai *postrouting*. Saat masuknya paket melalui *firewall*, *header* paket diperiksa oleh paket filter dan disesuaikan dengan peraturan yang ada [22]. *Firewall filtering* memeriksa setiap paket yang masuk dengan urutan aturan untuk menentukan apakah harus diblokir atau dikirim [23].

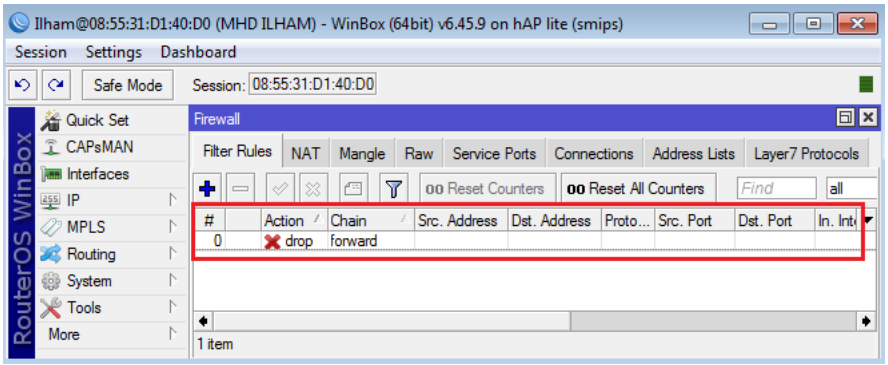
Cara Kerja Port Knocking

Metode keamanan jaringan komputer yang dikenal sebagai port knocking digunakan untuk menyembunyikan port yang biasanya terbuka dalam firewall [24]. Port knocking akan melakukan penutupan pada port yang tersedia sehingga pengguna tertentu saja yang memiliki hak untuk membuat akses port tersebut dapat mengaksesnya dengan mengetuk terlebih dahulu. Sebaliknya, pemilik hak untuk mengakses port tersebut tidak dapat melakukannya lagi dikarenakan *firewall* telah menutup semua port tanpa memperhatikan siapapun [25]. Hal ini dapat mencegah diketahuinya oleh pemindai apa saja layanan yang saat ini tersedia di host dan berfungsi sebagai perlindungan terhadap serangan *zero-day* [26]. Firewall akan membuat file log untuk mendeteksi apakah host sudah melakukan upaya koneksi atau tidak, car ini merupakan mekanisme dari *port knocking* [27]. FTP (File Transfer Protokol), SSH (Secure Shell), Telnet (Jaringan Telekomunikasi, API, Winbox, dan layanan WebFig pada router) dilindungi dengan pengetukan port ini [28]. Metode *port knocking* meningkatkan keamanan sistem, tetapi tidak menjamin keamanan sepenuhnya [29].

Implementasi

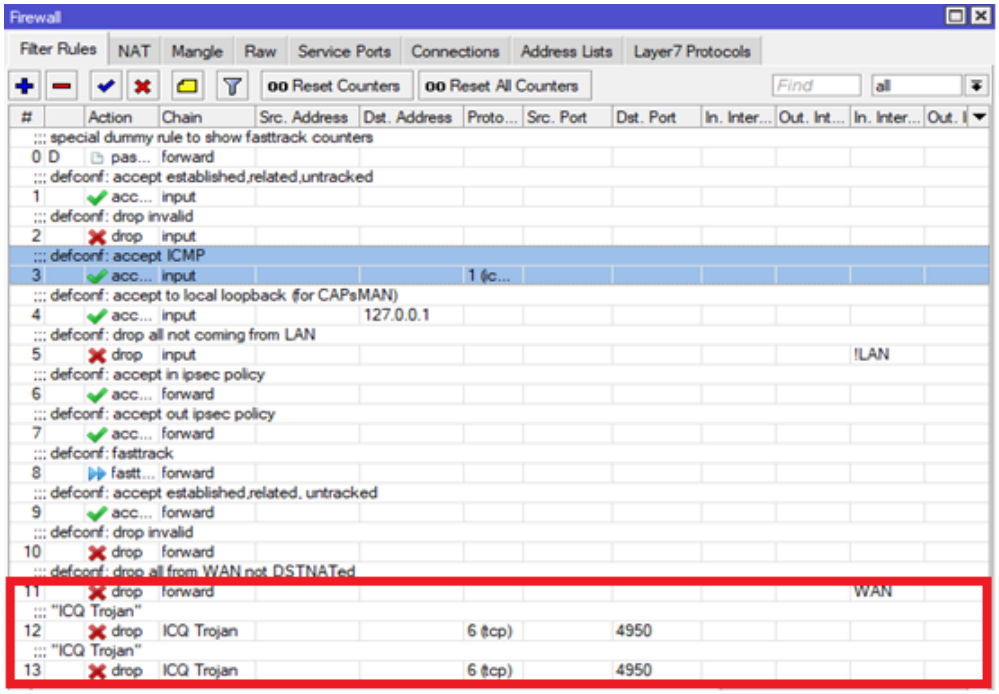
Implementasi ini kami ambil berdasarkan artikel yang relevan sebagai pendukung untuk menyelesaikan penelitian yang kami buat.

1. Login ke *board router* Mikrotik. Kemudian buka aplikasi winbox dan pilih kolom koneksi. Pilih alamat Mac yang akan digunakan. Step berikutnya adalah membuat aturan pada filter. Kemudian Langkah selanjutnya yaitu dengan memilih tombo; *filter rules* dan tekan tombol yang + yang berwarna biru dibagian bawah *filter rules.* Selanjutnya adalah dengan mengatur pengaturan yang ada di *filter rules* kemudian *general* dan *action* [30]. Dibawah ini merupakan hasil dari *filter rules*.



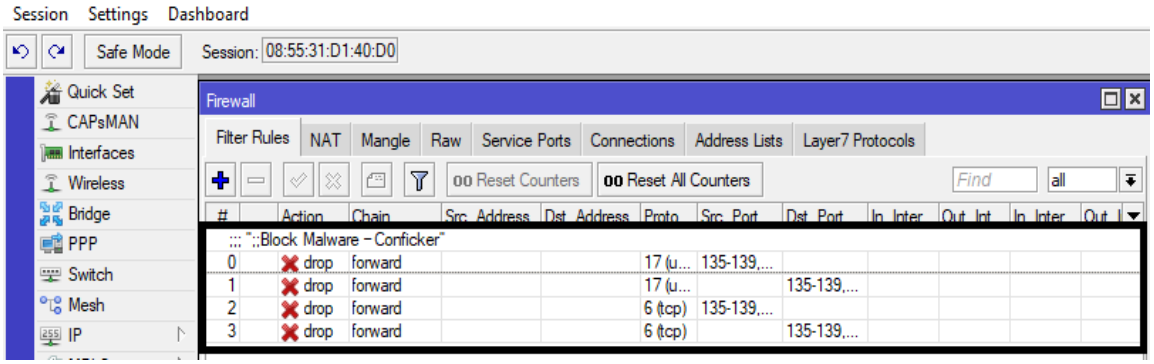
Gambar 2. Hasil *filter rules*

2. Langkah yang kedua ialah dengan mengatur pengaturan *firewall*. Cara untuk melakukan konfigurasi *firewall* menggunakan nama virus, *protokol*, dan juga *port*. Metode ini biasa digunakan dengan memberikan perinah / ip *Firewall Filter* add chain = ICQ Trojan Protocol = tcp dst-port = 4950 action = drop comment = "ICQ Trojan", dari metode tersebut menunjukkan hasil bahwa *malware* ada di tiap orang ataupun *device* komputer yang digunakan [30].



Gambar 3. Hasil *firewall rule block*

3. Pengaturan *Firewall Block Malware Conficker.* Pilih *Filter Rules,* lalu click add (+) berwarna biru, kemudian akan muncul *window* baru seperti gambar berikut. Kemudian pilih *general* dengan mengganti *Chain: forward, Protocol: 17 (udp), Src. Port: 135-139.445, Comment;;Block W32 Conficker*, klik OK kemudian menggunakan *Action drop*. Hasil pemblokiran *malware* tersebut dikumpulkan, dan hasilnya tampak seperti pada gambar berikut [30].



Gambar 4. *Firewall block malware*

4. Kesimpulan

Dapat disimpulkan bahwa metode-metode yang digunakan pada penelitian ini terbukti efektif dalam meningkatkan keamanan jaringan. *Firewall filtering* mampu memblokir serangan dari luar jaringan begitu pula dengan *port knocking*. Metode penelitian yang digunakan meliputi literature review dan seleksi studi, yang memberikan dukungan terhadap efektivitas metode keamanan tersebut melalui referensi ke artikel-artikel terkait. Dengan demikian, penelitian ini memberikan kontribusi penting dalam memperkuat keamanan jaringan mikrotik melalui penerapan *firewall filtering* dan *port knocking*.

Ucapan Terimakasih

Penulis mengucapkan terimakasih kepada Bapak Fauzan Prasetyo selaku dosen mata kuliah jaringan komputer karena telah membantu mendanai publikasi pada artikel ini.

Daftar Rujukan

[1] N. Haidar, F. P. Eka Putra, M. Arifin, M. Yasir Zain, and I. Darmawan, "Desain dan Perancangan Smart Campus berbasis ZigBee Wireless Sensor Network," *J. Inov. Teknol. dan Edukasi Tek.*, vol. 1, no. 11, pp. 842–850, 2021, doi: 10.17977/um068v1i112021p842-850.

[2] F. Prasetyo Eka Putra, "Sleep Mode: Strategi Efisiensi Wireless Sensor Network," *Informatics Educ. Prof. J. Informatics*, vol. 8, no. 1, pp. 52–56, 2023.
[3] N. Haidar Hari, F. P. Eka Putra, U. Hasanah, S. R. Sutarsih, and Riyan, "Transformasi Jaringan Telekomunikasi dengan Teknologi 5G: Tantangan, Potensi, dan Implikasi," *J. Inf. dan Teknol.*, vol. 5, no. 2, pp. 146–150, 2023, doi: 10.37034/jidt.v5i2.357.
[4] K. Al Fikri and Djuniadi, "Keamanan Jaringan Menggunakan Switch Port Security," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 5, no. 2, pp. 302–307, 2021, [Online]. Available: http://bit.ly/InfoTekJar
[5] A. Bustami and S. Bahri, "Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi : Systematic Review," *Unistek*, vol. 7, no. 2, pp. 59–70, 2020, doi: 10.33592/unistek.v7i2.645.
[6] F. P. E. Putra, D. A. M. Putra, A. Firdaus, and ..., "Analisis Kecepatan Dan Kinerja Jaringan 5G (generasi ke 5) Pada Wilayah Perkotaan," *... J. Informatics*, vol. 8, no. 1, pp. 47–51, 2023, [Online]. Available: http://ejournal-binainsani.ac.id/index.php/ITBI/article/view/2439%0Ahttp://ejournal-binainsani.ac.id/index.php/ITBI/article/download/2439/1631
[7] A. Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *J. Teknoinfo*, vol. 12, no. 2, p. 72, 2018, doi: 10.33365/jti.v12i2.121.
[8] Prayogi Wicaksana, F. Hadi, and Aulia Fitrul Hadi, "Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan," *J. KomtekInfo*, vol. 8, no. 3, pp. 169–175, 2021, doi: 10.35134/komtekinfo.v8i3.128.
[9] B. Jaya, Y. Yuhandri, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," *J. Sistim Inf. dan Teknol.*, vol. 2, pp. 115–123, 2020, doi: 10.37034/jsisfotek.v2i4.32.
[10] A. M. L. - AMIK BSI Purwokerto and Y. B. - AMIK BSI Purwokerto, "Analisis Sistem Pengelolaan, Pemeliharaan dan Keamanan Jaringan Internet Pada IT Telkom Purwokerto," *Evolusi J. Sains dan Manaj.*, vol. 6, no. 2, pp. 49–56, 2018, doi: 10.31294/evolusi.v6i2.4427.
[11] A. H. Fauzan Prasetyo Eka Putra, Selly Mellyana Dewi, Maugfiroh, "Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi," *J. Sistim Inf. dan Teknol.*, vol. 5, no. 2, pp. 26–32, 2023, doi: 10.37034/jsisfotek.v5i1.232.
[12] R. O. Nitra and M. Ryansyah, "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen," *J. Sist. dan Teknol. Inf.*, vol. 7, no. 1, p. 52, 2019, doi: 10.26418/justin.v7i1.29979.
[13] F. JAIDI, "A Quantified Trust-Risk Assessment Approach for Enhancing Firewalls-Filtering Services.," *J. Inf. Assur. \& Secur.*, vol. 14, no. 2, pp. 30–39, 2019.
[14] A. Robbahul Barra, R. Sujatmika, and I. Umami, "Sistem Keamanan Jaringan Komputer Bridge Firewall Menggunakan Router Board Mikrotik Rb750," *J. Teknol. Dan Sist. Inf. Bisnis-JTEKSIS*, vol. 4, no. 1, p. 427, 2022, [Online]. Available: https://doi.org/10.47233/jteksis.v4i2.561
[15] H. R. A. Krisna, "Implementasi Manajemen Bandwidth Menggunakan Mikrotik Pada Kantor Kesatuan Bangsa Dan Politik Kabupaten …," pp. 37–46, 2022.
[16] B. F. Audrey, "… Network Menggunakan Point To Point Tunnel Protocol Berbasis Mikrotik: Virtual Private Network Menggunakan Point To Point Tunnel Protocol Berbasis Mikrotik," *J. Netw. Comput. Appl. (ISSN …*, vol. 1, no. 1, pp. 1–8, 2022, [Online]. Available: http://jurnal.netplg.com/index.php/jnca/article/view/1
[17] M. Idhom, H. E. Wahanani, and A. Fauzi, "Network Security Applications Using the Port Knocking Method," *J. Phys. Conf. Ser.*, vol. 1569, no. 2, 2020, doi: 10.1088/1742-6596/1569/2/022046.
[18] A. Saputro, N. Saputro, and H. Wijayanto, "Metode Demilitarized Zone dan Port Knocking untuk Keamanan Jaringan Komputer," *CyberSecurity dan Forensik Digit.*, vol. 3, no. 2, pp. 22–27, 2020.
[19] N. A. Santoso, K. B. Affandi, and R. D. Kurniawan, "Implementasi Keamanan Jaringan Menggunakan Port Knocking," *J. Janitra Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 90–95, 2022, doi: 10.25008/janitra.v2i2.156.
[20] Astrid Noviriandini, Hermanto Hermanto, Diah Ayu Ambarsari, and Didy Eriawan, "Analisis Management Bandwidth Dan Firewall Dengan Router Mikrotik Pada Pt. Bca Multifinance," *J. Tek. dan Sci.*, vol. 1, no. 3, pp. 40–45, 2022, doi: 10.56127/jts.v1i3.466.
[21] A. Maulana, N. Suharto, and A. Hariyadi, "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*, vol. 13, no. 1, pp. 81–86, 2023, doi: 10.33795/jartel.v13i1.547.
[22] B. L. et al. Hoffman, "Analisi Jaringan & Design," *J. Tek. Ind. Mesin, Elektro dan Ilmu Komput.*, vol. 10, no. 1, pp. 15–20, 2019.
[23] L. Durante, L. Seno, and A. Valenzano, "A formal model and technique to redistribute the packet filtering load in multiple firewall networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2637–2651, 2021, doi: 10.1109/TIFS.2021.3057552.
[24] Muhammad Nur *et al.*, "The Effectiveness of the Port Knocking Method in Computer Security," *Int. J. Integr. Sci.*, vol. 2, no. 6, pp. 873–880, 2023, doi: 10.55927/ijis.v2i6.4526.
[25] P. Riska, P. Sugiartawan, and I. Wiratama, "Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking," *J. Sist. Inf. dan Komput. Terap. Indones.*, vol. 1, no. 2, pp. 53–64, 2018, doi: 10.33173/jsikti.12.
[26] Iwan Giri Waluyo and D. Kurniawan, "Mikrotik Login Security with Port-Knocking and Brute Force Firewall at PT. Time Excelindo," *Int. J. Integr. Sci.*, vol. 2, no. 7, pp. 971–978, 2023, doi: 10.55927/ijis.v2i7.4782.
[27] Yudi mulyanto, M. Julkarnain, and A. Jabi Afahar, "Implementasi Port Knocking Untuk Keamanan Jaringan Smkn 1 Sumbawa Besar," *J. Inform. Teknol. dan Sains*, vol. 3, no. 2, pp. 326–335, 2021, doi: 10.51401/jinteks.v3i2.1016.
[28] Mursyidah *et al.*, "Analysis and implementation of the Port Knocking method using Firewall-based Mikrotik RouterOS," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 536, no. 1, 2019, doi: 10.1088/1757-899X/536/1/012129.
[29] R. M. Arifianto, "An SSH Honeypot Architecture Using Port Knocking and Intrusion Detection System," *2018 6th Int. Conf. Inf. Commun. Technol.*, vol. 0, no. c, pp. 409–415, 2018.

[30] Andri, I. Gunawan, and I. O. Kirana, "Optimasi Sistem Keamanan Jaringan Komputer Terhadap Serangan Malware Menggunakan Filtering Firewall dengan Metode Port Blocking Optimization of Computer Network Security System Against Malware Attacks Using Firewall Filtering with Port Blocking Method Art," *JOMLAI J. Mach. Learn. Artif. Intell.*, vol. 1, no. 2, pp. 2828–9099, 2022, doi: 10.55123/jomlai.v1i2.816.