

Optimizing Network Security Point to Point with ACL Filtering and TTL Methods

Mugi Raharjo^{1*}, Waeisul Bismi², Rachmat Adi Purnama³, Firmansyah⁴

¹Informatika, Universitas Nusa Mandiri
e-mail: ¹mugi.mou@nusamandiri.ac.id

^{2,3,4}Ilmu Komputer, Universitas Bina Sarana informatika
e-mail: ²waeisul.wbn@bsi.ac.id, ³rachmat.rap@bsi.ac.id, ⁴firmansyah.fmy@bsi.ac.id

Diterima	Direvisi	Disetujui
31-08-2023	01-11-2023	01-12-2023

Abstrak - Keamanan pada jaringan komputer merupakan suatu hal yang wajib dimiliki di era saat ini. Penelitian ini membahas tentang optimalisasi keamanan jaringan titik ke titik menggunakan metode *filtering ACL* (*Access Control List*) dan pendekatan *Time To Live (TTL)*. Keamanan jaringan menjadi isu kritis dalam lingkungan digital yang terus berkembang, terutama pada komunikasi titik ke titik yang memerlukan perlindungan data yang efektif. Dalam konteks ini, penelitian ini bertujuan untuk meningkatkan keamanan komunikasi dengan mengintegrasikan dua pendekatan utama, yaitu *filtering ACL* dan pengaturan *TTL*. Studi ini pertama-tama menganalisis mekanisme kerja *ACL* dalam mengontrol lalu lintas jaringan berdasarkan aturan yang ditentukan sebelumnya. Selanjutnya, pendekatan *TTL* dieksplorasi untuk mengatur batasan usia paket data, meminimalkan risiko serangan jaringan seperti serangan ping berlebihan. Melalui serangkaian percobaan dan simulasi, kinerja metode keamanan yang diusulkan dievaluasi dengan mempertimbangkan faktor-faktor seperti latensi, *throughput*, dan efisiensi jaringan. Hasilnya menunjukkan bahwa kombinasi *filtering ACL* dan pendekatan *TTL* secara signifikan meningkatkan keamanan jaringan titik ke titik. Latensi tetap dalam rentang yang dapat diterima sementara tingkat serangan berkurang secara signifikan. Penelitian ini memberikan keberhasilan mengamankan jaringan point to point yang sudah dilakukan pengamanan dengan metode *ACL* dan *TLL*. Pada dasarnya dari hasil ini Perusahaan akan diuntungkan dengan optimalnya jaringan dan keamanan mereka.

Kata Kunci: Keamanan Jaringan, *ACL*, *Time to Live*

Abstract - Security in computer networks is a mandatory aspect in the current era. This research discusses the optimization of point-to-point network security using the *ACL* (*Access Control List*) filtering method and the *Time To Live (TTL)* approach. Network security has become a critical issue in the evolving digital environment, especially in point-to-point communications that require effective data protection. In this context, the research aims to enhance communication security by integrating two main approaches, which are *filtering ACL* and *TTL* settings. This study first analyzes how *ACL* works in controlling network traffic based on predefined rules. Next, the *TTL* approach is explored to set the packet data's age limit, minimizing the risk of network attacks such as excessive ping attacks. Through a series of experiments and simulations, the proposed security method's performance is evaluated, considering factors like latency, *throughput*, and network efficiency. The results show that the combination of *filtering ACL* and *TTL* approach significantly enhances point-to-point network security. Latency remains within an acceptable range, while the attack rate decreases significantly. This research successfully secures point-to-point networks that have been previously secured using *ACL* and *TTL* methods. Essentially, these results benefit the company by optimizing their network and security.

Keywords: Network Security, *ACL*, *Time to Live*

PENDAHULUAN

Dalam penelitian ini, kami dilatar belakangi pada masalah keamanan dan kurang optimalnya sistem yang sedang berjalan pada Perusahaan. Dalam masalahnya sering terjadi pembobolan akses internet tanpa seizin pemilik, Untuk itu peneliti melakukan Analisa terkait kebutuhan atau solusi yang ditawarkan terhadap permasalahan tersebut. Penelitian bertujuan untuk mengoptimalkan keamanan jaringan komputer melalui penggunaan *ACL Filtering* dan metode Akses *Time To Live* dengan penerapan melalui perangkat Mikrotik. Keamanan jaringan adalah aspek krusial dalam memastikan integritas, kerahasiaan, dan ketersediaan data serta layanan yang disediakan oleh jaringan. Dengan ancaman siber yang terus berkembang, pendekatan preventif seperti pengaturan akses yang ketat dan pengelolaan lalu lintas yang bijaksana menjadi semakin penting. (Rathore, Sharma, Loia, Jeong, & Park, 2017) Kami juga mendiskusikan solusi pertahanan mutakhir yang dapat melindungi pengguna jaringan sosial dari ancaman ini. Kami kemudian menyajikan arah masa depan, Menurut Indah Kusuma dalam penelitiannya (Astuti, 2018) Jaringan komputer (jaringan) adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. (Sumardi & Zaen, 2018) Perkembangan dunia jaringan komputer sangat cepat, semua komputer diharapkan dapat berkomunikasi satu dengan yang lain dengan medium tertentu. (Amarudin & Riskiono, 2019) Pesatnya perkembangan teknologi internet tidak dapat dipungkiri akan berdampak pada meningkatnya *cyber crime*. (Aji, Fadlil, & Riadi, 2017) *Mikrotik Router* adalah salah satu sistem operasi yang dapat digunakan sebagai router jaringan yang handal, mencakup berbagai fitur lengkap untuk jaringan. (Aji et al., 2017) Efek utama dari serangan jaringan komputer berupa lambatnya akses internet. Selain itu untuk jenis serangan jaringan yang sangat berbahaya dapat mengakibatkan rusaknya data pada server, sehingga hal ini sangat merugikan pengguna ataupun *end user* yang sedang mengakses. Kegiatan merusak, mengganggu, mencuri data, dan segala hal yang merugikan pemilik server pada jaringan komputer adalah suatu tindak ilegal dan dapat dijatuhkan sanksi secara hukum di pengadilan. Memerangi kejahatan internet telah menjadi porsi utama bagi agen-agen penegak hukum dan intelejen, baik nasional maupun internasional, tanpa kecuali para praktisi bisnis, sampai kepada para pelanggan, dan *end user*.

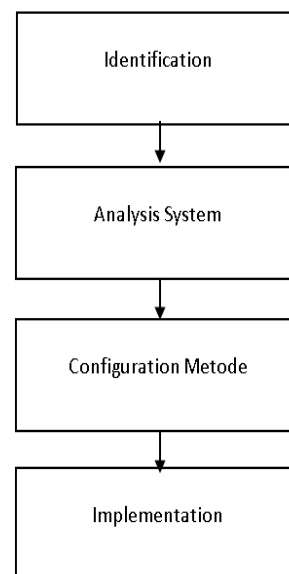
Berdasarkan penelitian dari (Rahayu et al., 2023) Sistem keamanan pada jaringan dibutuhkan untuk pembatasan privilege level jaringan luar mengakses server dan melakukan *blocking* terhadap *traffic* network yang dianggap sangat berbahaya pada jaringan internal Perusahaan. (Simanjuntak,

Suharyanto, & Jamilah, 2017) *Router* menyediakan kemampuan untuk menyaring *traffic*, seperti memblokir *traffic* Internet, dengan *Access Control Lists (ACL)*. *ACL* adalah suatu rentetan list dari suatu statemen perijinan atau penolakan yang di aplikasikan kepada alamat-alamat jaringan atau layer protokol paling atas. (Sihotang, Sumarno, & Damanik, 2020) penerapan *Access Control List (ACL)* untuk mengatur hak akses tiap perangkat yang ada di dalam jaringan tersebut. *Access Control List (ACL)* dapat menyaring lalu lintas data suatu jaringan dengan mengontrol apakah paket-paket tersebut dilewatkan atau dihentikan. Jaringan dibangun menggunakan dengan beberapa perangkat jaringan yang berbeda – beda, salah satunya adalah router. *Router* merupakan alat yang dapat memproses paket data berbeda jaringan (antar jaringan) melalui proses yang disebut dengan routing. banyak sekali perusahaan yang memproduksi router.

(Moura, Heidemann, Schmidt, & Hardaker, 2019) *TTL* ditentukan di beberap zona pada *router*, dan resolusi *DNS* harus memperhatikan keamanan. Makalah ini memberikan evaluasi cermat pertama tentang bagaimana berbagai faktor yang saling berinteraksi ini memengaruhi masa pakai cache yang efektif. (Sharif Hossen, Masum Billah, & Yasmin, 2018) Oleh karena itu, kami akan menyelidiki routing yang efisien untuk mengubah *TTL* dan ukuran *buffer* sangat penting untuk kinerja jaringan secara keseluruhan.

METODE PENELITIAN

Dalam penelitian ini kami membuat kerangka kerja dalam menganlisi dan menemukan solusi pada permasalahan keamanan jaringan.



Sumber : Hasil Penelitian (2023)

Gambar. 1 Kerangka Penelitian

Berikut penjelasan mengenai kerangka kerja yang kami lakukan :

1. Identification

Tahapan pertama dalam penelitian ini dibagi menjadi dua bagian identifikasi yaitu kebutuhan perangkat Identifikasi juga dapat disebut dengan perencanaan pengumpulan data. (Hidayat, Malau, Setiadi, & Julianto, 2023). Kami melakukan identifikasi kebutuhan pada Perusahaan demi menjaga keamanan pada jaringan komputernya.

2. Analysis System

Penguraian dari suatu sistem informasi yang utuh kedalam bagian-bagian komponennya dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan, kesempatan, hambatan yang terjadi dan kebutuhan yang dihadapakan sehingga dapat diusulkan perbaikan (Coker et al., 2018). Pada tahapan ini kami menganalisis kebutuhan pada jaringan yang telah kami identifikasi permasalahannya, kemudian kami temukan sebuah solusi menggunakan metode yang tepat.

3. Configuration Methode

Pada tahapan ini kami melakukan konfigurasi terhadap router sesuai dengan temuan masalah dan hasil analisis yang kami lakukan yaitu dengan mengkonfigurasi *ACL* dan *TTL* pada jaringan point to point sehingga tingkat keamanan pada sistemjaringan ini mejadi lebih aman

4. Implementasi

Implementasi merupakan suatu rangkaian aktifitas dalam rangka menghantarkan kebijakan kepada masyarakat sehingga kebijakan tersebut dapat membawa hasil sebagaimana diharapkan. (Novan Mamoto, 2018). Pada tahapan implementasi ini kami melakukan test tingkat keberhasilan dari konfigurasi yang telah dilakukan mengukur sejauh mana keamanan yang tercapai pada hasil ujicoba.

HASIL DAN PEMBAHASAN

Pengujian dan simulasi yang dilakukan dalam penelitian ini menghasilkan temuan yang signifikan terkait dengan efektivitas integrasi metode *filtering ACL* dan pendekatan *Time To Live (TTL)* dalam meningkatkan keamanan jaringan titik ke titik. Hasil-hasil utama meliputi:

1. Peningkatan Keamanan

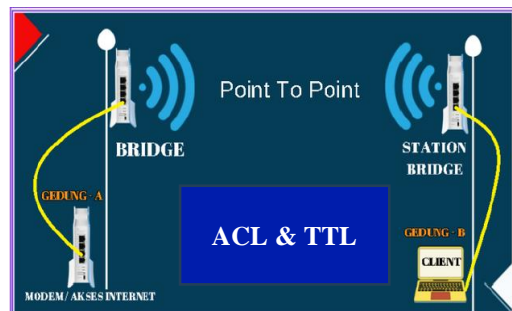
Integrasi *filtering ACL* dan pendekatan *TTL* mampu mengurangi tingkat serangan jaringan yang dihadapi oleh komunikasi titik ke titik. Pengaturan aturan *ACL* dan pengendalian *TTL* berdampak positif terhadap peningkatan tingkat keamanan secara keseluruhan.

2. Pengurangan Serangan Ping Berlebihan

Pendekatan *TTL* membuktikan efektivitasnya dalam mengurangi serangan ping berlebihan yang dapat merusak kinerja jaringan. Dengan membatasi usia paket data, serangan semacam itu dapat diatasi.

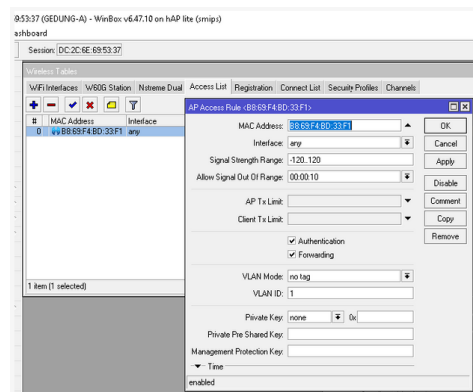
3. Pengaruh Terhadap Kinerja Jaringan

Meskipun ada penambahan lapisan keamanan, pengujian menunjukkan bahwa peningkatan keamanan ini hanya memiliki dampak minimal terhadap kinerja jaringan. Latensi tetap dalam batas yang dapat diterima, dan throughput tidak mengalami penurunan yang signifikan.



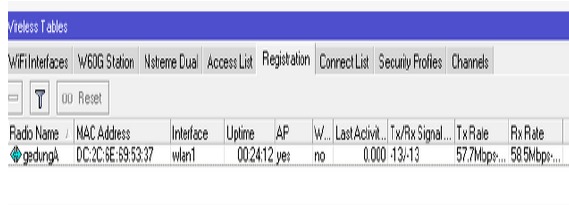
Sumber : Hasil Penelitian (2023)
Gambar 2. Skema Jaringan

Fitur Access List (ACL) pada perangkat MikroTik adalah alat yang memungkinkan Anda mengendalikan dan mengatur lalu lintas jaringan berdasarkan aturan-aturan yang ditentukan. *ACL* digunakan untuk mengizinkan atau memblokir paket data yang melewati perangkat jaringan berdasarkan kriteria tertentu.



Sumber : Hasil Penelitian (2023)
Gambar 3. Konfigurasi *Accesslist*

Pada tahapan ini kami mendaftarkan identitas pada router yang akan terkoneksi yaitu pada Gedung-B dengan memasukkan Alamat *MAC-ADDRESS* beserta *signal-strength* yang berfungsi untuk membatasi koneksi dengan jarak tertentu pada router mikrotik.



Radio Name	MAC Address	Interface	Uptime	AP	W..	Last Activ...	Tx/Rx Signal...	Tx Rate	Rx Rate
gedungk	DC:2C:9E:69:53:37	wlan1	00:24:12:yer	no	0.000	131:13	57.7Mbps...	58.5Mbps...	

Sumber : Hasil Penelitian (2023)

Gambar 4. Konektivitas Antar Gedung

Pada tahap ini dapat dipastikan bahwa hanya Gedung-B yang dapat terkoneksi dengan Gedung-A sebab sudah didaftarkan identitas berupa *MAC-ADDRESS* pada router Gedung-A.

```
.. Move up one level
/command Use command at the base level
[admin@GEDUNG-B] > ping google.com
SEQ HOST                               SIZE TTL TIME STATUS
0 74.125.200.100                       56 1 51ms
1 74.125.200.100                       56 1 56ms
2 74.125.200.100                       56 1 40ms
3 74.125.200.100                       56 1 42ms
```

Sumber : Hasil Penelitian (2023)

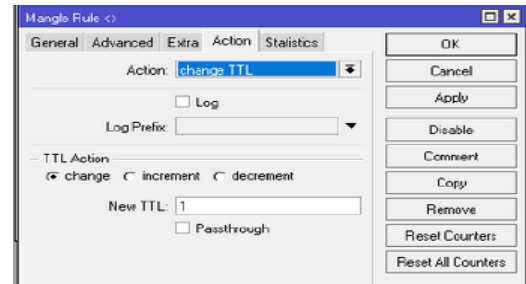
Gambar 5. Hasil Ping Test

Dalam tahapan penginstalasian pada tahapan test koneksi dapat dilakukan dengan cara melakukan ping test antar router atau antar client dari kedua jaringan yang berbeda.

Time To Live (TTL) adalah nilai yang ada dalam header paket *IP (Internet Protocol)* yang menunjukkan berapa lama paket tersebut diizinkan untuk berada dalam jaringan sebelum dihapus atau dibuang oleh *router* atau perangkat jaringan lainnya. *TTL* awalnya diperkenalkan sebagai mekanisme untuk mencegah paket-paket yang hilang atau terjebak secara permanen dalam jaringan.

Ketika sebuah paket data dikirim melalui jaringan, setiap router atau hop yang dilewati oleh paket tersebut akan mengurangi nilai *TTL* sebelum mengirimkan paket tersebut lebih lanjut. Ketika nilai *TTL* mencapai nol, *router* akan membuang paket tersebut dan mengirimkan pesan *ICMP (Internet Control Message Protocol)* ke pengirim untuk

memberi tahu bahwa paket telah dihapus karena *TTL* telah habis.

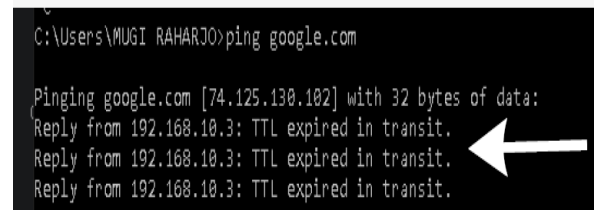


Sumber : Hasil Penelitian (2023)

Gambar 6. Konfigurasi *Time To Live*

Dalam tahap konfigurasi ini kami mengubah nilai pada *TTL* menjadi 1 yang akan mengakibatkan terbatasnya nilai *TTL* yang akan diterima oleh klien sehingga klien atau *router* yang terkoneksi tidak akan bisa meneruskan paket Kembali kepada user atau *router* lainnya.

```
/command Use command at the base level
[admin@GEDUNG-B] > ping google.com
SEQ HOST                               SIZE TTL TIME STATUS
0 142.250.4.101                         56 1 40ms
1 142.250.4.101                         56 1 148ms
2 142.250.4.101                         56 1 47ms
sent=3 received=3 packet-loss=0% min-rtt=40ms avg-rtt=78ms max-rtt=148ms
[admin@GEDUNG-B] >
```

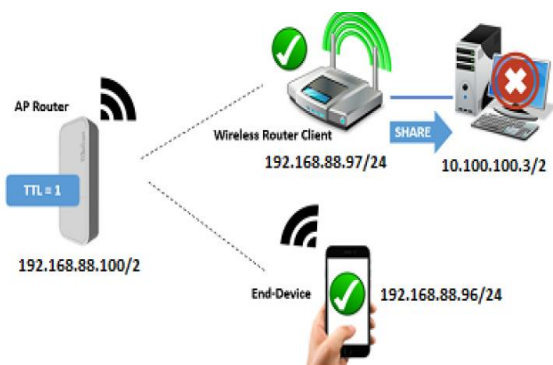


Sumber : Hasil Penelitian

Gambar 7. Hasil test pada konfigurasi *TTL*

Pada tahapan testing yang kami lakukan jaringan berhasil dilakukan *TTL* dengan menunjukkan nilai pada *TTL* yaitu '1' dan *TTL Expired in Transit* pada sisi client. Sehingga dapat dipastikan dari sisi keamanan bahwa seorang client atau router tidak bisa lagi meneruskan paket tersebut. Hal ini sangat membantu dalam pencegahan terjadi pencurian akses pada jaringan yang dimiliki oleh Perusahaan, karna seperti diketahui pencurian akses dapat terjadi kapanpun dan dimanapun yang dapat mengakibatkan terjadinya pembobolan data dan penggunaan internet berlebih yang menjadikan jaringan menjadi lambat sehingga tidak efektif lagi dalam penggunaan jaringan diperusahaan. Pencegahan ini juga bisa

menghindari terjadinya penyebaran virus atau malware dari pihak yang tidak dikenal.



Sumber : citraweb.com

Gambar 7. Simulasi TTL

Garis besar dari konfigurasi adalah kita akan mengubah nilai TTL (Time To Live) dari packet download yang menuju ke client. Disini nanti kita akan merubahnya menjadi nilai '1'. Untuk di Mikrotik sendiri kita bisa melakukan konfigurasi tersebut pada menu firewall mangle.

KESIMPULAN

Dalam era di mana konektivitas dan pertukaran data semakin mendominasi, perlindungan terhadap integritas dan kerahasiaan informasi menjadi esensial. Penelitian ini telah membahas tentang optimalisasi keamanan jaringan titik ke titik dengan mengintegrasikan metode filtering ACL (Access Control List) dan pendekatan Time To Live (TTL). Melalui serangkaian uji coba dan simulasi, penelitian ini berhasil mengidentifikasi dampak positif dari pendekatan yang diusulkan terhadap keamanan dan kinerja jaringan.

Hasil penelitian menunjukkan bahwa penggunaan kombinasi filtering ACL dan pendekatan TTL secara signifikan meningkatkan keamanan komunikasi titik ke titik. Integrasi ACL memungkinkan pengontrolan lalu lintas yang lebih ketat, sementara pengaturan TTL memberikan perlindungan terhadap serangan ping berlebihan dan mengurangi risiko overload jaringan. Meskipun ditemukan peningkatan dalam keamanan, dampak terhadap kinerja jaringan tetap dalam batas yang dapat diterima.

Penelitian ini memberikan pemahaman yang lebih dalam tentang bagaimana dua metode keamanan ini dapat saling berintegrasi untuk menciptakan lapisan perlindungan yang lebih kokoh dalam komunikasi titik ke titik. Meskipun demikian, masih ada potensi pengembangan lebih lanjut, termasuk eksplorasi lebih mendalam tentang skenario penggunaan yang

berbeda, konfigurasi yang lebih canggih, dan dampak pada jaringan yang lebih besar dan kompleks.

Dengan demikian, penelitian ini memberikan sumbangan penting terhadap pengembangan praktik terbaik dalam mengamankan komunikasi jaringan titik ke titik. Diharapkan temuan dari penelitian ini akan memberikan panduan berharga bagi profesional keamanan jaringan dan peneliti untuk terus meningkatkan infrastruktur keamanan di lingkungan yang terus berubah dan semakin kompleks.

REFERENSI

- Aji, S., Fadlil, A., & Riadi, I. (2017). Pengembangan Sistem Pengaman Jaring. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, 3(1), 11.
- Amarudin, A., & Riskiono, S. D. (2019). Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (Vpn). *Jurnal Teknoinfo*, 13(2), 100. <https://doi.org/10.33365/jti.v13i2.309>
- Astuti, I. K. (2018). Fakultas Komputer INDAH KUSUMA ASTUTI Section 01. *Jaringan Komputer*, 8.
- Coker, C., Greene, E., Shao, J., Enclave, D., Tula, R., Marg, R., ... Tang, S. (2018). No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析Title. *Transcommunication*, 53(1), 1–8. Retrieved from <http://www.tfd.org.tw/opencms/english/about/background.html%0Ahttp://dx.doi.org/10.1016/j.cirp.2016.06.001%0Ahttp://dx.doi.org/10.1016/j.powtec.2016.12.055%0Ahttps://doi.org/10.1016/j.ijfatigue.2019.02.006%0Ahttps://doi.org/10.1016/j.matlet.2019.04.024%0Aht>
- Hidayat, W. F., Malau, Y., Setiadi, A., & Julianto, M. F. (2023). Konfigurasi dan Implementasi OwnCloud Sebagai Cloud Storage. *Jurnal Infortech*, 5(1), 83–87. <https://doi.org/10.31294/infortech.v5i1.15836>
- Informatika, J., Perancangan, D. A. N., Jips, S., Aura, V. F., Maksimalisasi, T., Jaringan, K., ... Utara, S. (2023). Jurnal informatika dan perancangan sistem (jips), 5(1), 37–44.
- Moura, G. C. M., Heidemann, J., Schmidt, R. de O., & Hardaker, W. (2019). Cache me if you can: Effects of DNS time-to-live. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, (1), 101–115. <https://doi.org/10.1145/3355369.3355568>
- Novan Mamoto, I. S. dan G. U. (2018). Implementasi Pembangunan Infrastruktur Desa Dalam Penggunaan Dana Desa Tahun 2017 (Studi) Desa Ongkaw Ii Kecamatan Sinonsayang

- Kabupaten Minahasa Selatan. *Jurusan Ilmu Pemerintahan*, 1(1), 1–11.
- Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, 421, 43–69. <https://doi.org/10.1016/j.ins.2017.08.063>
- Sharif Hossen, M., Masum Billah, M., & Yasmin, S. (2018). Impact of buffer size and TTL on DTN routing protocols in intermittently connected mobile networks. *International Journal of Engineering & Technology*, 7(3), 1735. <https://doi.org/10.14419/ijet.v7i3.14122>
- Sihotang, B. K., Sumarno, S., & Damanik, B. E. (2020). Implementasi Access Control List Pada Mikrotik dalam Mengamankan Koneksi Internet Koperasi Sumber Dana Mutiara. *JURIKOM (Jurnal Riset Komputer)*, 7(2), 229. <https://doi.org/10.30865/jurikom.v7i2.2010>
- Simanjuntak, P., Suharyanto, C. E., & Jamilah. (2017). Analisis Penggunaan Access Control List (Acl) Dalam Jaringan Komputer Di Kawasan. *Isd*, 2(2), 122–128.
- Sumardi, S., & Zaen, M. T. A. (2018). Perancangan Jaringan Komputer Berbasis Mikrotik Router OS Pada SMAN 4 Praya. *Jurnal Informatika Dan Rekayasa Elektronik*, 1(1), 50. <https://doi.org/10.36595/jire.v1i1.32>