JAMBURA JOURNAL OF INFORMATICS
Volume 5, No. 2 | October 2023, 108-119
ISSN 2685-4244, doi: 10.37905/jji. v5i2.20415

Penerapan *firewall* di router OS mikrotik pada aplikasi e-rapor

Aditya Nugraha Hairun, Muhammad Rifai Katili, Rahman Takdir, Mohamad Syafri Tuloli

Program Studi Sistem Informasi, Universitas Negeri Gorontalo, Indonesia

Riwayat Artikel:
Diterima 12 Juni 2023
Direvisi 11 September 2023
Disetujui 29 Oktober 2023
Diterbitkan 31 Oktober 2023

Kata Kunci:
Denial of service
e-rapor
Firewall
Keamanan jaringan
Mikrotik

ABSTRACT. The e-Rapor is an additional app/tool for teachers and educational units to report student learning outcomes to submit to students' parents or guardians. However, the apps remain to show weakness in the application at SMA Negeri 1 Gorontalo, particularly about network security where Denial of Service (DoS) attacks, which will cause an increase in resources on the server, thereby increasing the load on the e-Rapor. This research aimed to apply a firewall on the Mikrotik OS Router to anticipate DoS attacks. The development process employed the Network Development Life Cycle (NDLC) method, a process approach in data communication that describes the initial and final cycles of building a computer network. This research result indicates that the firewall in the quarantine router os mikrotik can do IP address to DoS on e-Rapor in 80-90% of applications.

ABSTRAK. Aplikasi e-Rapor merupakan opsi alat bantu bagi guru dan satuan pendidikan melakukan pelaporan hasil belajar peserta didik untuk disampaikan kepada orang tua atau wali murid. Namun dalam penerapannya di SMA Negeri 1 Gorontalo aplikasi e-Rapor masih terdapat kekurangan yakni pada keamanan jaringan yaitu serangan berupa *Denial of Service* (*DoS*) yang akan menyebabkan bertambahnya *resource* pada server sehingga meningkatkan beban terhadap *server* aplikasi e-Rapor. Penelitian ini bertujuan untuk melakukan penerapan *firewall* yang terdapat di router OS Mikrotik guna mengantisipasi serangan DoS. Proses pengembangan menggunakan metode *Network Development Life Cycle* (*NDLC*). NDLC adalah salah satu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang awal dan akhirnya dalam membangun sebuah jaringan komputer. Hasil penelitian ini menunjukkan bahwa firewall yang terdapat pada Router OS Mikrotik dapat melakukan karantina terhadap *IP address* yang melakukan DoS pada aplikasi e-Rapor sebesar 80-90%.

Penulis Korespondensi:
Aditya Nugraha Hairun
Universitas Negeri Gorontalo
Jl Jendral Sudirman No 6, Kota Gorontalo, Indonesia.
Email: aditya_s1sisfo2018@mahasiswa.ung.ac.id

PENDAHULUAN

Pada saat ini perkembangan teknologi informasi sangat pesat. Fasilitas internet tersedia dan dapat dimanfaatkan untuk berbagai kepentingan organisasi. Namjn demikian, selalu terdapat celah yang dialami oleh pengguna internet seperti serangan dari pihak-pihak yang tidak bertanggung jawab atau sering disebut dengan *hacker* (Purba & Efendi, 2020). Seiring dengan perkembangan revolusi industri 4.0, kebutuhan akan informasi yang cepat dan akurat semakin meningkat (Yoga & Ardhana, 2022). Selain tingginya manfaat yang dirasakan, tingkat risiko dan ancaman penyalahgunaan teknologi informasi juga semakin tinggi dan kompleks (Bustami & Bahri, 2020). Keamanan jaringan komputer merupakan bagian sebuah sistem yang sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi pengguna dari mana dan kapan saja (Fachri & Harahap, 2020). Antisipasi perlu dilakukan terhadap bahaya virus atau malware yang dapat menyebabkan kerusakan pada komputer, server atau jaringan komputer (Gunawan dkk., 2021).

Keamanan pada suatu jaringan sangat mutlak dibutuhkan karena rawannya jaringan apabila terhubung dengan jaringan luar (WAN) dimana pencurian sabotase pada jaringan, penyalahgunaan jaringan *wireless* serta *trojan* atau *rootkit* masih marak terjadi (Yassin, 2020). Keamanan siber merupakan sebuah rangkaian aktivitas yang diarahkan untuk melindungi dari ancaman, gangguan, serangan jaringan komputer (perangkat keras dan perangkat lunak) terkait informasi didalamnya, dan elemen-elemen ruang siber lainnya (Aji, 2023). Dalam konteks negara dan pertahanan perkembangan teknologi informasi diikuti oleh potensi ancaman dalam bidang keamanan siber pada negara (Razzaq dkk., 2022).

Perkembangan teknologi informasi dalam sistem pendidikan bersifat fleksibel tanpa dibatasi oleh ruang dan waktu (Zainuddin, 2021). Aplikasi e-Rapor dalam penggunaannya dengan cara diinstall pada sebuah komputer yang dijadikan sebagai server e-Rapor, dan diakses melalui jaringan baik secara lokal maupun online, namun dalam penggunaannya e-Rapor sering mendapat akses yang banyak diluar dari jumlah pengguna yang seharusnya, serangan tersebut berupa *Denial Of Service* (DoS). Sistem pertahanan terhadap *server* masih banyak yang tergantung secara manual kepada administrator sehingga membuat integritas sistem tergantung pada ketersediaan dan kecepatan administrator dalam merespon gangguan terjadi (Stephani dkk., 2020). Serangan dunia maya yang terjadi beragam mulai dari serangan *malware*, SSH, dan serangan berbasis web, hal ini membuat prioritas pengamanan dan pemantauan data infrastruktur jaringan harus ditingkatkan (Putra dkk., 2022).

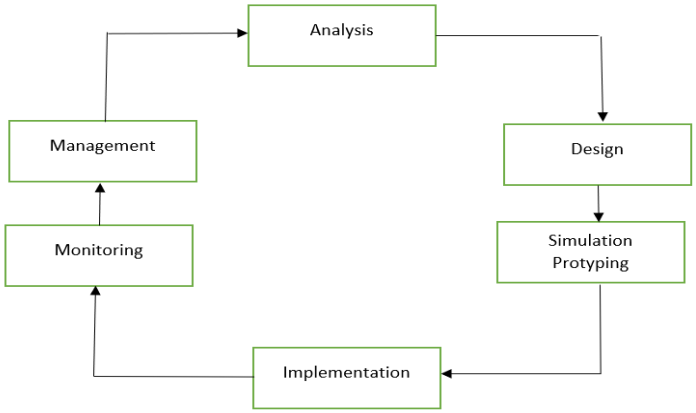
Sistem komputer menjadi bagian yang sangat penting dan tidak dapat dipisahkan dalam dunia pendidikan (Dermawati & Hasim Siregar, 2020). Mikrotik merupakan sistem operasi router, yang di-rilis dengan nama mikrotik Router OS yang mampu diinstall pada *hardware* tertentu. Routerboard Mikrotik adalah salah satu vendor baik hardware dan software yang menyediakan fasilitas untuk sebuah router. Mikrotik Router OS bisa difungsikan baik sebagai *server* maupun *client* atau bahkan keduanya bersama dalam satu mesin yang sama, fitur termasuk dalam *package* (Dewi dkk., 2020). Mikrotik merupakan perangkat keras yang memiliki fitur sangat lengkap, penggunaan mikrotik pada sebuah jaringan sangatlah baik, karena mikrotik mempunyai fitur firewall yang berfungsi untuk memeriksa dan menentukan apakah sebuah paket data yang dapat keluar atau masuk dari sebuah jaringan (Rahmat dkk., 2021). Mikrotik dapat digunakan untuk mengatur *bandwith*, mengatur *firewall*, mengatur notifikasi masalah jaringan, mengatur monitoring jaringan maupun *tunneling* (Gamaliel dkk., 2022). Terkait dengan fakta-fakta di atas dan adanya potensi serangan terhadap penggunaan e-Rapor, penelitian ini dilakukan dengan tujuan untuk melakukan penerapan firewall yang terdapat di router OS Mikrotik guna mengantisipasi serangan DoS pada aplikasi e-Rapor di SMA Negeri 1 Gorontalo.

METODE

Penelitian ini menggunakan metode pengembangan *Network Development Life Cycle* (NDLC). NDLC adalah salah satu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang awal dan akhirnya dalam membangun sebuah jaringan komputer (Rodianto dkk, 2022; Sanjaya dan Setiadi, 2019). Pendekatan ini terdiri atas tahapan, yaitu: *analysis, design, simulation prototype, implementation*, monitoring dan *management* (Gambar 1).

Pada tahap awal yakni **Analisis** dilakukan dengan menganalisis topologi serta konfigurasi yang telah berjalan pada Router OS Mikrotik dan Server e-Rapor. Selanjutnya berdasarkan hasil analisis sebelumnya dilakukan proses **Desain** konfigurasi firewall yang akan digunakan. Kemudian dilakukan **Simulasi prototype** hasil desain. Pada tahap ini dilakukan pengembangan jaringan dalam bentuk simulasi menggunakan aplikasi yang bertujuan untuk mensimulasikan prototipe. **Implementasi** protype merupakan tahap dilaksanakannya implementasi dari konfigurasi firewall yang telah didesain

sebelumnya. Langkah ini akan melibatkan konfigurasi Router OS Mikrotik menggunakan aplikasi WinBox. Setelah proses implementasi selesai, dilanjutkan dengan tahapan **Monitoring** untuk memastikan bahwa jaringan dan komunikasi berjalan sesuai dengan tujuan yang telah ditetapkan. Pada tahap **Manajemen** dilakukan aktivitas terkait pemeliharaan dan pengelolaan. Dalam hal ini, kebijakan perlu dibuat untuk menjadikan dan mengatur sistem yang telah dibangun berjalan dengan baik dan unsur reliability tetap terjaga.

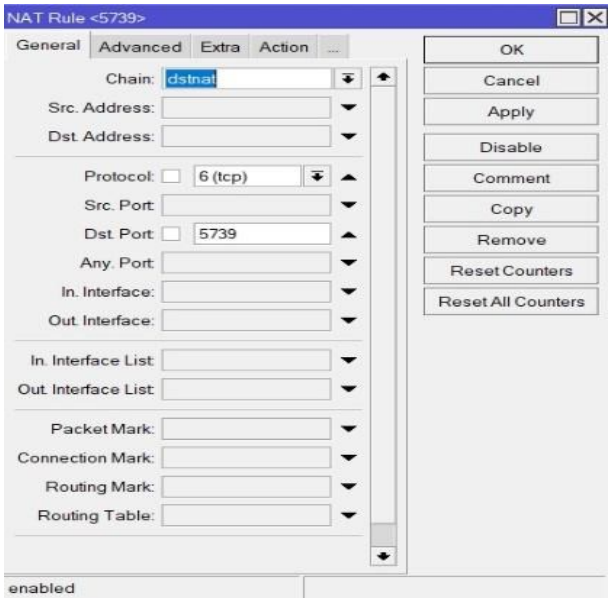


Gambar 1. Proses tahapan NDLC.

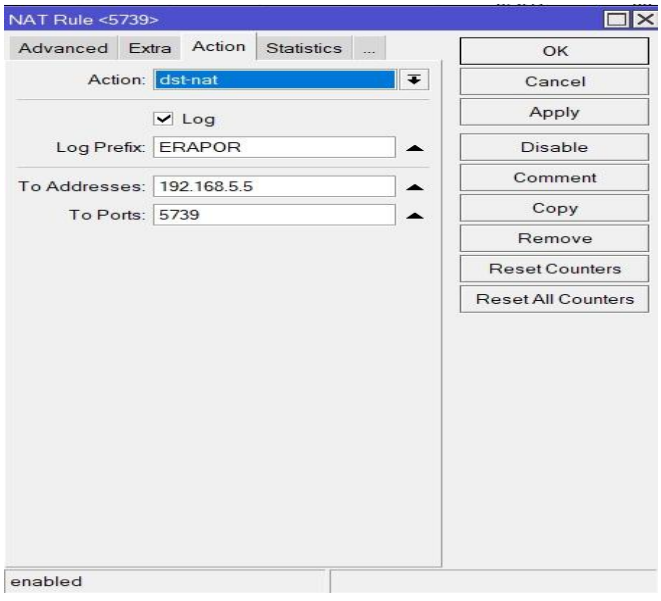
HASIL DAN DISKUSI

Konfigurasi NAT

NAT *(Network Address Translation)* adalah proses untuk memodifikasi sumber atau alamat tujuan dalam header IP dari sebuah paket saat sedang dalam transisi. Proses konfigurasi yang dilakukan yakni chain dstnat yakni pengalihan untuk paket data yang masuk ke dalam Router OS Mikrotik dengan *protocol* tcp dan menuju port 5739 seperti dapat dilihat pada Gambar 2. Adapun Gambar 3 mengarahkan jaringan yang masuk ke *port* 5739 ke *IP Address 192.168.5.5 port* 5739.



Gambar 2. Konfigurasi NAT e-Rapor tab general

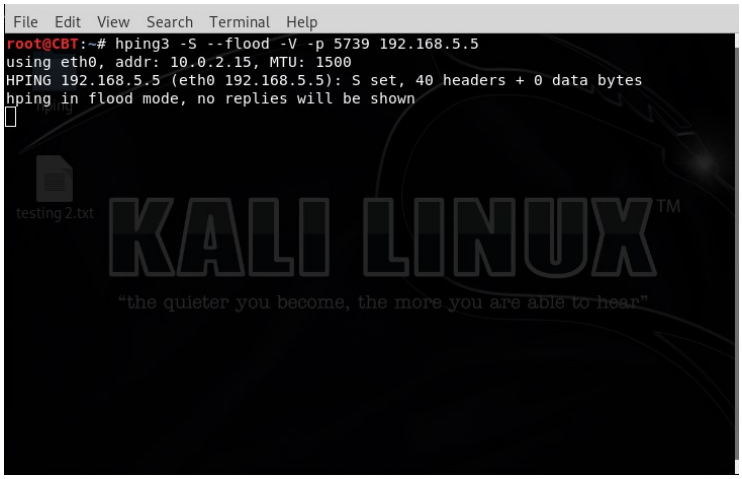


Gambar 3. Konfigurasi NAT e-Rapor tab action

Pengujian Serangan Denial of Service Sebelum Menggunakan Firewall

Serangan DoS dengan menggunakan aplikasi hping3, penjelasan terhadap serangan yang dilakukan yaitu (Gambar 4):

- hping3 yaitu perintah untuk menjalankan aplikasi hping3.
- -S --flood yaitu perintah untuk melakukan serangan *Syn Flood Attack*, serangan tersebut akan mengirimkan paket dengan volume tinggi.
- -V yaitu perintah untuk *Verbosity* yakni menampilkan hasil dari proses yang dijalankan.
- -p 5739 merupakan *port* yang menjadi target serangan.
- 5. 192.168.5.5 adalah *IP Address* yang menjadi target serangan.

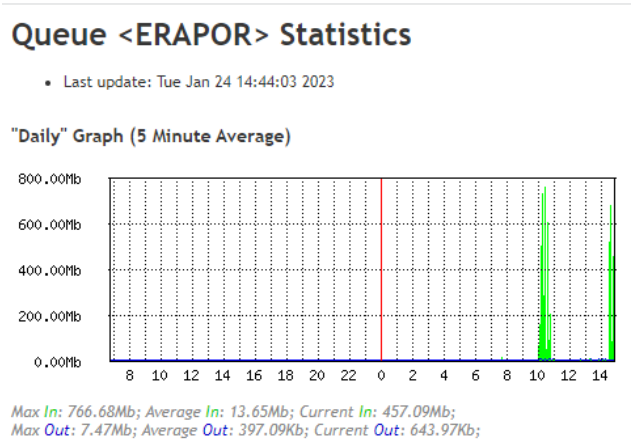


Gambar 4. Aplikasi hping3 untuk melakukan DoS

Gambar 5. Traffic pada server tanpa firewall Mikrotik

Trafik *download* dan *upload* pada server E-Rapor sebesar 11 Mbps dan 7.6 Mbps, yang berarti trafik memenuhi jaringan ke arah server E-Rapor sehingga server sulit untuk diakses. Hal ini mengakibatkan lalu lintas data menjadi terganggu seperti dapat dilihat pada Gambar 5.

Hasil dari MRTG sebelum dilakukan pemasangan *firewall* guna mengantisipasi serangan DoS dengan hasil *Max In*: 766.68 Mb dan *Max Out*: 7.47 Mb Berdasarkan hasil tersebut dapat dilihat bahwa aplikasi e-Rapor mendapatkan serangan yang cukup besar yaitu sebesar 766.68 Mb dalam waktu 5 menit. Hal ini tentu akan menyebabkan trafik dan *resource* server terbebani (Gambar 6). Untuk itu akan dilakukan proses konfigurasi *firewall* guna mengantisipasi serangan DoS.

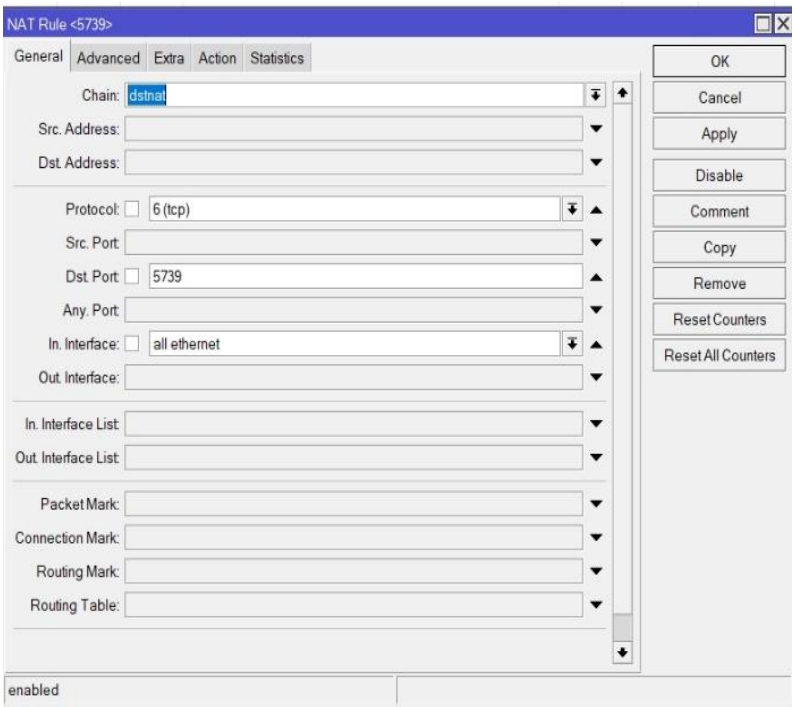


Gambar 6. Hasil MRTG sebelum konfigurasi firewall

Konfigurasi Firewall Guna Mengantisipasi Serangan Denial Of Service

Konfigurasi NAT Tab General

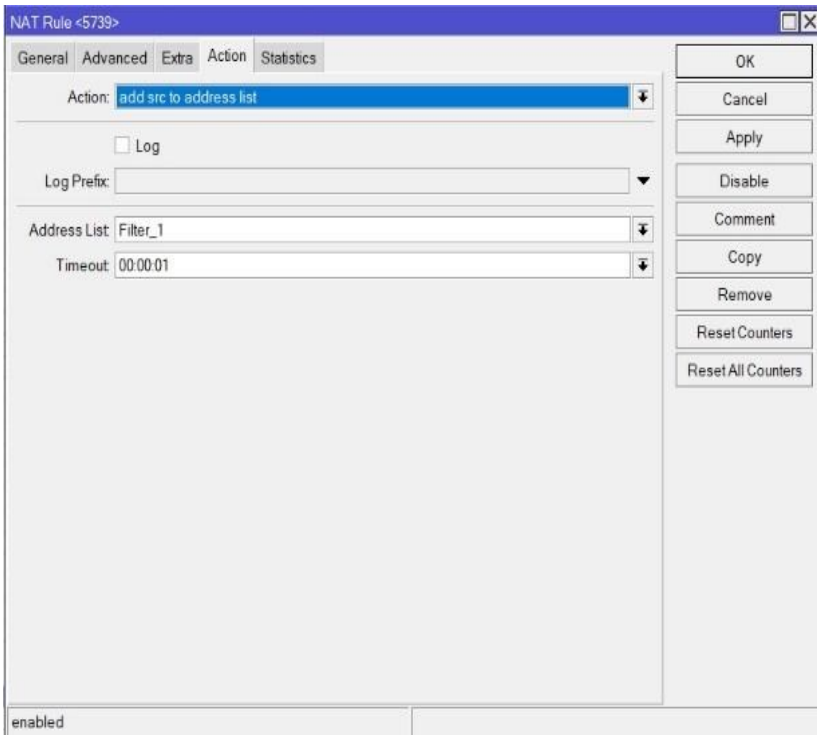
Pada bagian chain diisi dengan dstnat, protocol di isi dengan tcp, dst *port* di isi 5739 (Gambar 7).



Gambar 7. Menu tambah NAT tab general

Konfigurasi NAT Tab Action

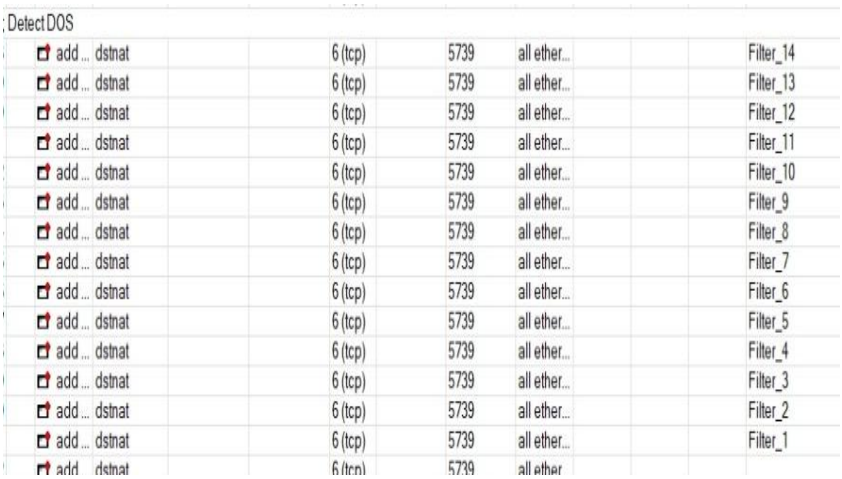
Pada bagian ini action diisi dengan *add src to address list*, bagian *Address List* di isi dengan Filter_1 serta timeout 00:00:01 selanjutnya klik OK untuk menyimpan konfigurasi pertama (Gambar 8).



Gambar 8. Menu tambah NAT Tab Action

Konfigurasi Lanjutan

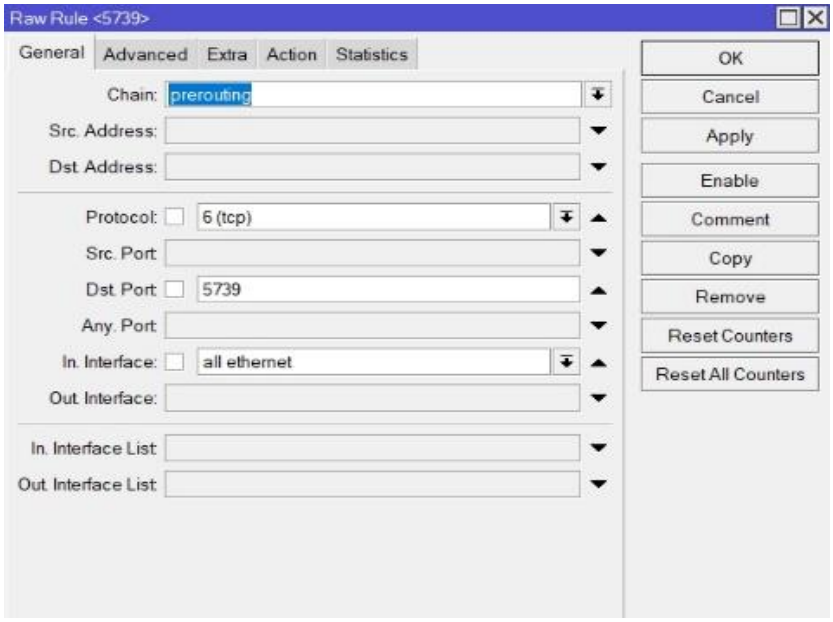
Konfigurasi yang dilakukan pada bagian 1–2 dan dilakukan sebanyak 15 kali. Hasilnya seperti pada Gambar 9.



Gambar 9. Tampilan konfigurasi firewall NAT

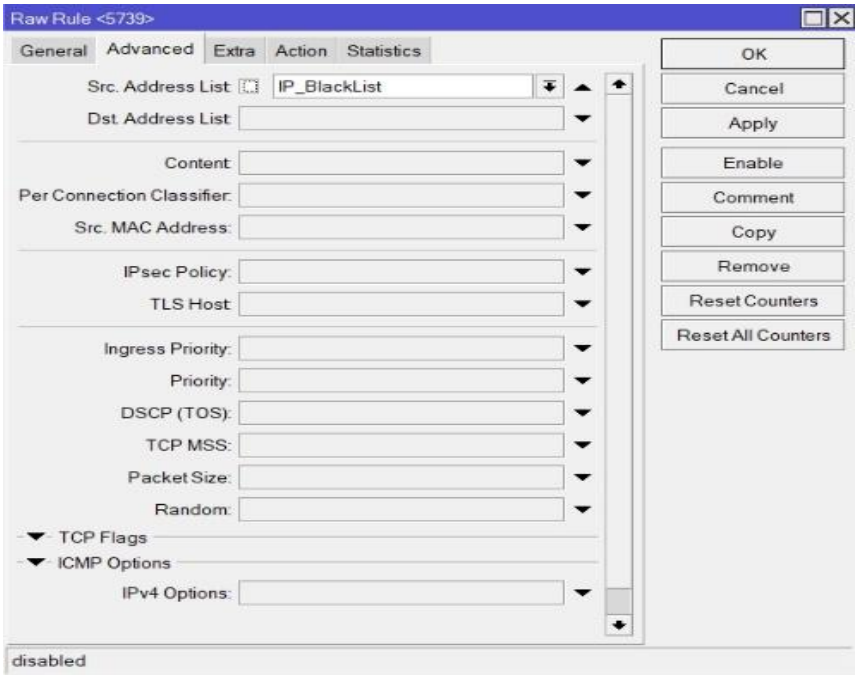
Konfigurasi Firewall RAW

Pada bagian *chain* di isi dengan prerouting, bagian *protocol* diisi dengan tcp, bagian dst port di isi dengan 5739 serta in interface di isi dengan *all ethernet*, dapat dilihat pada Gambar 10.



Gambar 10. Menu RAW tab general

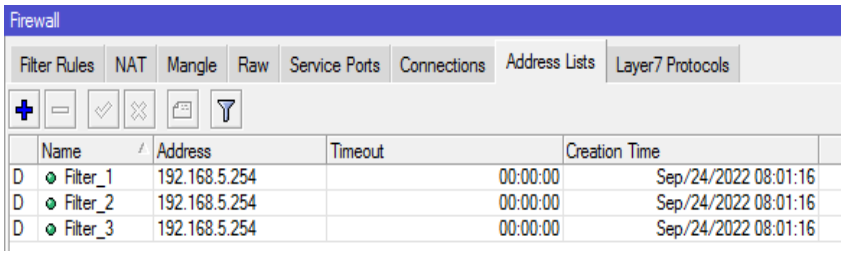
Pada tab *Advanced* pada bagian *Src.Address List* di isi dengan IP_BlackList, dapat dilihat di Gambar 11.



Gambar 11. Menu RAW tab advanced

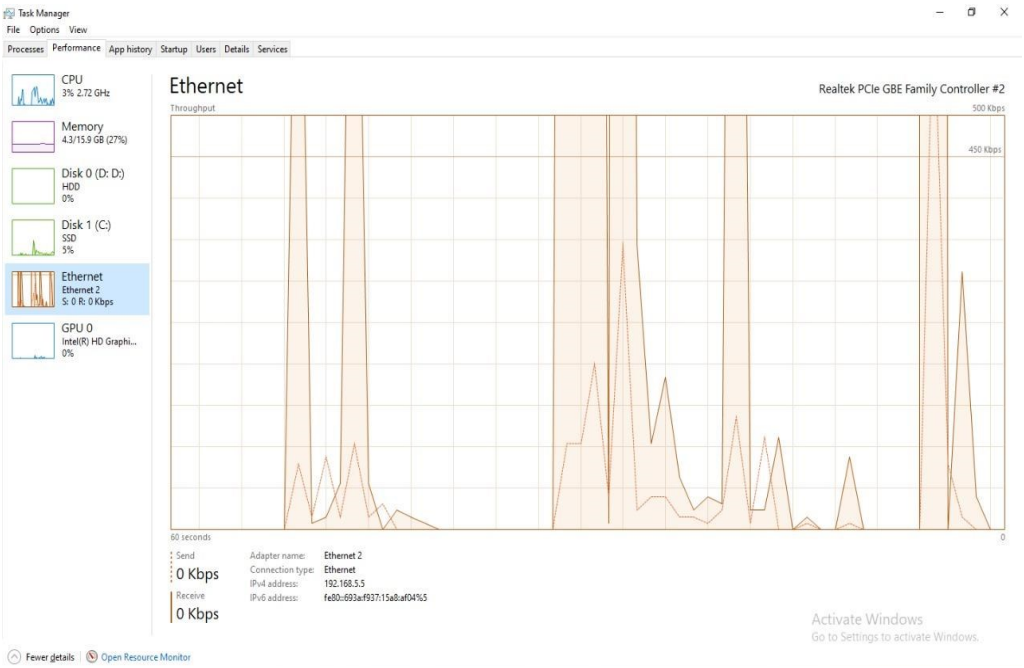
Pengujian Setelah Konfigurasi Firewall

Address Lists yang berfungsi mencatat IP Address yang melakukan akses ke port 5739, setiap IP Address akan diberikan nama sesuai dengan filter yang telah dilewati, dapat dilihat pada Gambar 12.

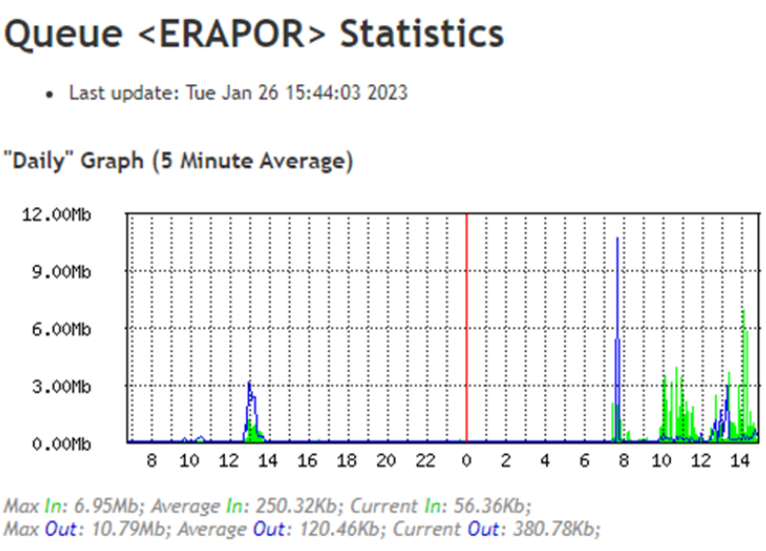


Gambar 12. Menu NAT firewall tab address lists

Pada resource server yang mengalami serangan DOS setelah dilakukan konfigurasi firewall berbeda dengan sebelum dilakukan konfigurasi firewall, dapat dilihat pada Gambar 13.



Gambar 13. Resource server di DoS setelah dipasang firewall

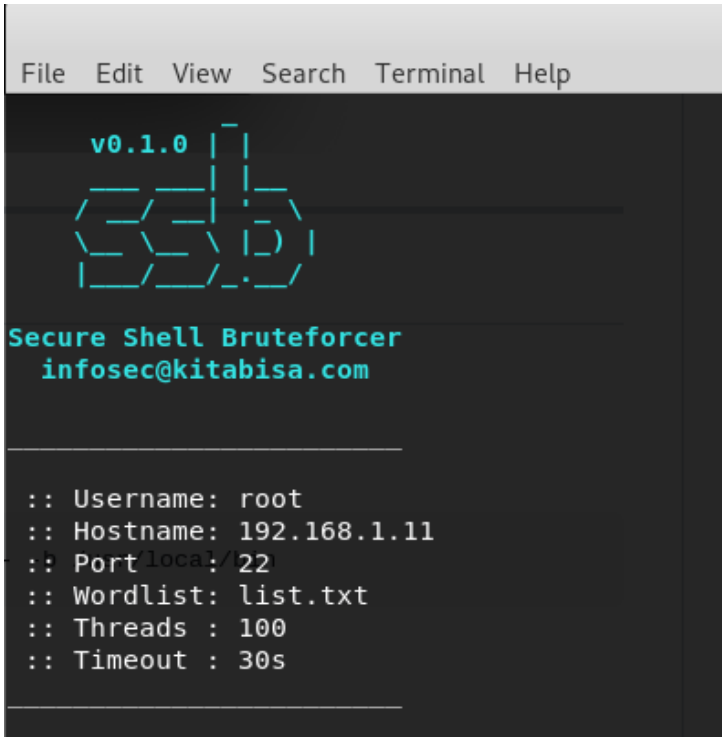


Gambar 14. Hasil MRTG setelah konfigurasi firewall

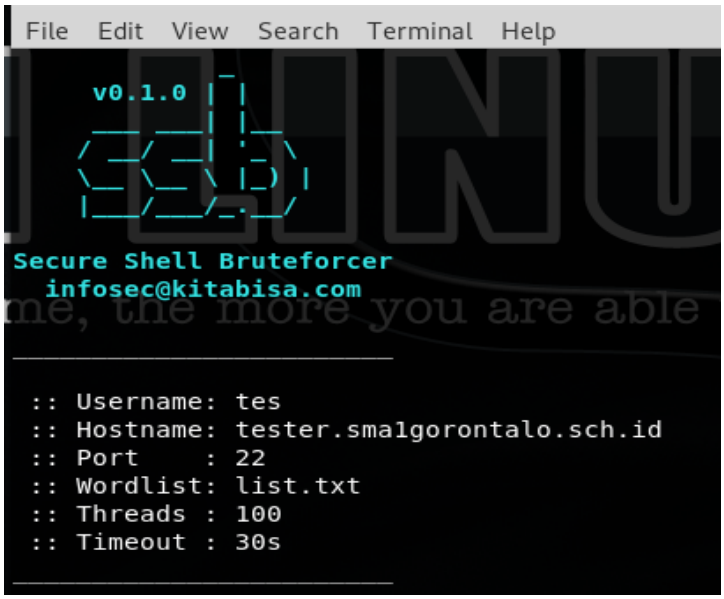
Hasil dari MRTG setelah dilakukan pemasangan firewall guna mengantisipasi serangan DoS dengan hasil Max In: 6.95 Mb dan Max Out: 10.79 Mb. Berdasarkan hasil tersebut dapat dilihat bahwa aplikasi e-Rapor dapat menahan serangan dengan paket yang masuk hanya sebesar 6.95 Mb serta paket yang keluar sebesar 10.79 Mb, dapat dilihat pada Gambar 14.

Pengujian Firewall Dengan Bentuk Serangan Lainnya

Firewall yang telah dikonfigurasi dilakukan pengujian menggunakan metode serangan yang berbeda yaitu melakukan serangan dengan metode *brute force* dan DoS Online.



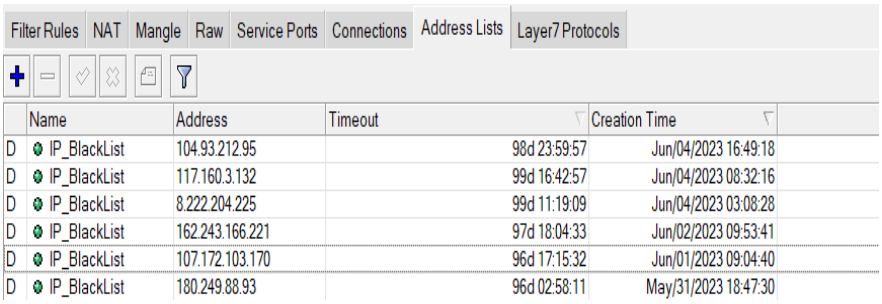
Gambar 15. Hasil MRTG setelah konfigurasi firewall



Gambar 16. Brute force online

Pada Gambar 15 dan 16 dilakukan pengujian dengan melakukan serangan brute force baik pada jaringan lokal maupun online, dengan hasil yang didapatkan, yaitu firewall dapat menahan serangan *brute force*.

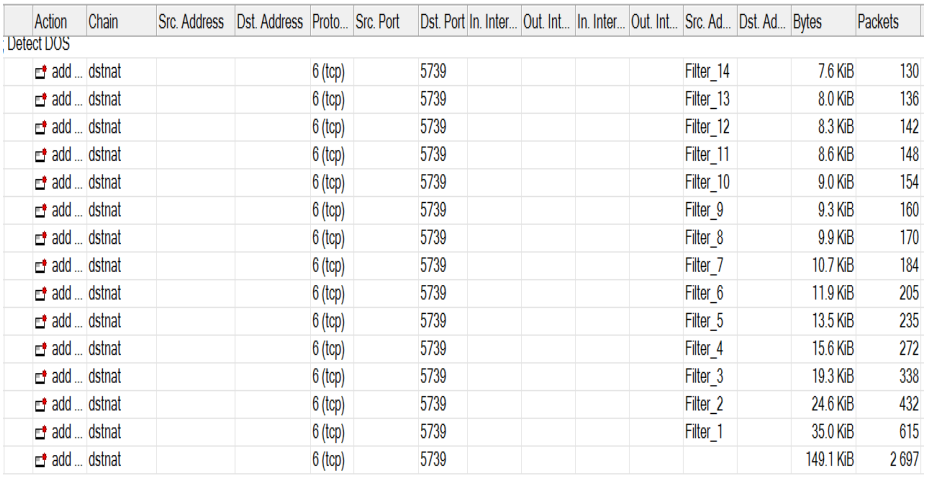
Gambar 17 merupakan daftar *IP Address* yang masuk dalam daftar blacklist karena melakukan serangan. Gambar 18 dan Gambar 19 merupakan trafik dari *rule firewall* NAT dan RAW yang telah dilakukan konfigurasi, dengan hasil masing-masing rule trafiknya rendah sehingga konfigurasi yang dilakukan tidak memberikan beban pada Router OS Mikrotik.



Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

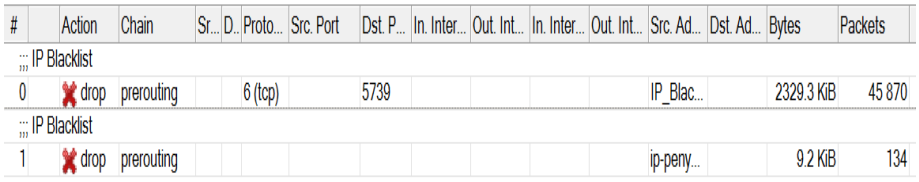
	Name	Address	Timeout	Creation Time
D	IP_BlackList	104.93.212.95	98d 23:59:57	Jun/04/2023 16:49:18
D	IP_BlackList	117.160.3.132	99d 16:42:57	Jun/04/2023 08:32:16
D	IP_BlackList	8.222.204.225	99d 11:19:09	Jun/04/2023 03:08:28
D	IP_BlackList	162.243.166.221	97d 18:04:33	Jun/02/2023 09:53:41
D	IP_BlackList	107.172.103.170	96d 17:15:32	Jun/01/2023 09:04:40
D	IP_BlackList	180.249.88.93	96d 02:58:11	May/31/2023 18:47:30

Gambar 17. List IP address blacklist



	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
;; Detect DOS															
	add ...	dstnat			6 (tcp)		5739					Filter_14		7.6 KiB	130
	add ...	dstnat			6 (tcp)		5739					Filter_13		8.0 KiB	136
	add ...	dstnat			6 (tcp)		5739					Filter_12		8.3 KiB	142
	add ...	dstnat			6 (tcp)		5739					Filter_11		8.6 KiB	148
	add ...	dstnat			6 (tcp)		5739					Filter_10		9.0 KiB	154
	add ...	dstnat			6 (tcp)		5739					Filter_9		9.3 KiB	160
	add ...	dstnat			6 (tcp)		5739					Filter_8		9.9 KiB	170
	add ...	dstnat			6 (tcp)		5739					Filter_7		10.7 KiB	184
	add ...	dstnat			6 (tcp)		5739					Filter_6		11.9 KiB	205
	add ...	dstnat			6 (tcp)		5739					Filter_5		13.5 KiB	235
	add ...	dstnat			6 (tcp)		5739					Filter_4		15.6 KiB	272
	add ...	dstnat			6 (tcp)		5739					Filter_3		19.3 KiB	338
	add ...	dstnat			6 (tcp)		5739					Filter_2		24.6 KiB	432
	add ...	dstnat			6 (tcp)		5739					Filter_1		35.0 KiB	615
	add ...	dstnat			6 (tcp)		5739							149.1 KiB	2 697

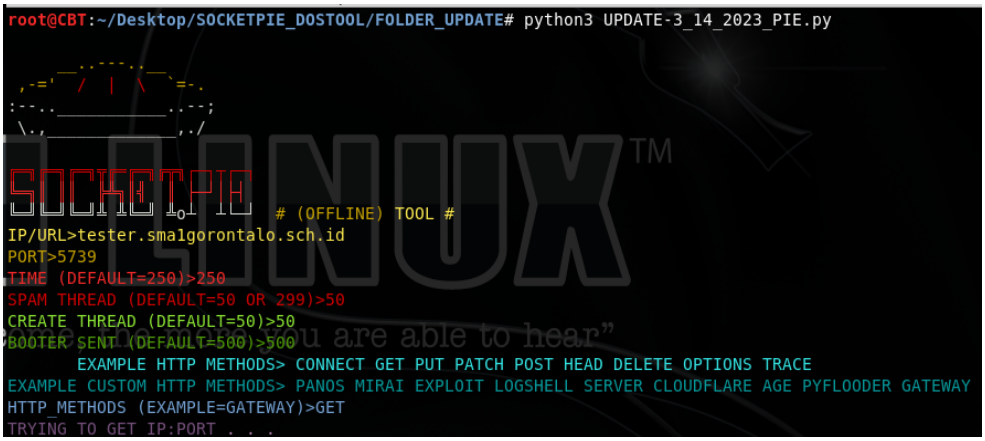
Gambar 18. Trafic rule firewall NAT



#		Action	Chain	Sr...	D...	Proto...	Src. Port	Dst. P...	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
;;; IP Blacklist																
0		drop	prerouting			6 (tcp)		5739					IP_Blac...		2329.3 KiB	45 870
;;; IP Blacklist																
1		drop	prerouting										ip-peny...		9.2 KiB	134

Gambar 19. Trafic rule firewall RAW

Gambar 20 merupakan proses pengujian DoS pada layer 7, dengan hasil aplikasi yang digunakan untuk melakukan serangan DoS, yaitu SOCKETPIE tidak dapat melakukan serangan disebabkan konfigurasi *firewall* yang telah dilakukan.



Gambar 20. DoS layer 7

Hasil Pengujian Firewall

Berdasarkan Tabel 1 dengan hasil dari *Max In* pada MRTG sebelum dilakukan konfigurasi *firewall* dengan hasil 766.68 Mb sedangkan setelah dilakukan konfigurasi firewall mendapatkan hasil 6.95 Mb hal ini tentu memberikan dampak yang besar terhadap trafik pada aplikasi yang mengalami DoS dimana sebelum dilakukan konfigurasi firewall trafik yang masuk tergolong cukup besar sehingga akan membebankan resource server maupun menghambat trafik pada jaringan e-Rapor.

Tabel 1. Hasil pengujian

Hasil	Sebelum Konfigurasi	Setelah Konfigurasi
Max In	766.68 Mb	6.95 Mb
Max average in	13.65 Mb	250.32 Kb
Current in	457.09 Mb	56.36 Kb
Max out	7.47 Mb	10.79 Mb
Average out	397.09 Kb	120.46 Kb
Current out	643.97 Kb	380.78 Kb

KESIMPULAN

Penelitian ini menghasilkan sebuah konfigurasi *firewall* yang dapat mengantisipasi serangan DoS pada aplikasi e-Rapor. Dengan adanya konfigurasi ini memudahkan admin jaringan dalam menghadapi serangan DoS yang terjadi, dapat dilihat pada Tabel 2 menunjukkan kemampuan Mikrotik yang telah dilakukan konfigurasi untuk mengurangi dampak dari serangan DoS yang terjadi, dengan perbandingan hasil sebelum dikonfigurasi dan sesudah dilakukan konfigurasi memiliki perbedaan yang cukup signifikan dalam mengantisipasi serangan DoS, sebelum dilakukan konfigurasi jumlah *Max In* pada Mikrotik sebesar 766,68 Mb sedangkan setelah dilakukan konfigurasi menjadi 6,95 Mb dengan hasil tersebut menunjukkan kemampuan dari konfigurasi yang telah dilakukan dapat mengantisipasi serangan DoS.

REFERENSI

Aji, M. P. (2023). Sistem keamanan siber dan kedaulatan data di Indonesia dalam perspektif ekonomi politik (studi kasus perlindungan data pribadi). *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *13*(2), 222–238. doi: 10.22212/jp.v13i2.3299

Bustami, A., & Bahri, S. (2020). Ancaman, serangan dan tindakan perlindungan pada keamanan jaringan atau sistem informasi: Systematic review. *Jurnal Pendidikan dan Aplikasi Industri (UNISTEK), 7*(2), 59-70. doi: 10.33592/unistek.v7i2.645

Dermawati, R., & Hasim Siregar, M. (2020). Implementasi honeypot pada jaringan internet labor fakultas teknik Uniks menggunakan dionaea sebagai keamanan jaringan. *Jurnal Ilmiah Edutic, 7*(1). doi: 10.21107/edutic.v7i1.8660

Dewi, S., Riyadi, F., Suwastitaratu, T., & Hikmah, N. (2020). Keamanan jaringan menggunakan VPN (*Virtual Private Network*) dengan metode PPTP (*Point To Point Tunneling Protocol*) pada kantor desa Kertaraharja Ciamis. *Jurnal Sains dan Manajemen*, *8*(1). doi: 10.31294/evolusi.v8i1.7658

Fachri, B., & Harahap, F. H. (2020). Simulasi penggunaan intrusion detection system *Intrusion Detection System* (IDS) sebagai keamanan jaringan dan komputer. *Jurnal Media Informatika Budidarma*, *4*(2), 413-420. doi: 10.30865/mib.v4i2.2037

Gamaliel, F., Yudi, P., & Arliyanto, D. (2022). Perancangan manajemen jaringan komputer berbasis mikrotik dengan menggunakan top down network design. *Jurnal Informatika & Rekayasa Elektronika). 5*(2). 230-243. doi: 10.36595/jire.v5i2.693

Gunawan, A. R., Sastra, N. P., & Wiharta, D. M. (2021). Penerapan keamanan jaringan menggunakan sistem snort dan honeypot sebagai pendeteksi dan pencegah malware. *Majalah Ilmiah Teknologi Elektro*, *20*(1), 81. doi: 10.24843/mite.2021.v20i01.p09

Purba, W. W., & Efendi, R. (2020). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *AITI: Jurnal Teknologi Informasi*, *17*, 143–158. doi: 10.24246/aiti.v17i2.143-158

Putra, W. R. A., Nurwa, A. R. A., Priambodo, D. F., & Hasbi, M. (2022). Infrastructure as code for security automation and network infrastructure monitoring. *Matrik: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, *22*(1), 203–217. doi: 10.30812/matrik.v22i1.2471

Putri, A. W. O. K., Aditya, A. R. Musthofa, D. L., & Widodo, P. (2022). Serangan hacking tools sebagai ancaman siber dalam sistem pertahanan negara (studi kasus: predator). *Global Political Studies Journal*, *6*(1). 35-46. doi: 10.34010/gpsjournal.v6i1

Rahmat, N. M., Gulo, P., Suherdi, D., & Rezky, S. F. (2021). Pemanfaatan firewall pada jaringan mengunakan Mikrotik RB951Ui-2HnD. *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD*, *4*(2), 173–179. doi: 10.53513/jsk.v4i2.3304

Rodianto., Idham., Yuliadi., Zaen, M. T. A., & Ramadhan, W. (2022). Penerapan network development life cycle (NDLC) dalam pengembangan jaringan komputer pada Badan Pengelolaan Keuangan dan Aset Daerah (BPKAD) provinsi NTB. *Jurnal Ilmiah FIFO*, XIV (1), 35-46. doi: 10.22441/fifo.2022.v14i1.004

Sanjaya, T. & Setiyadi, D. (2019). Network development life cycle (NDLC) dalam perancangan jaringan komputer pada rumah shalom mahanaim. *Jurnal Mahasiswa Bina Insani*, *4*(1), 1-10.

Stephani, E., Nova, F., Asri, E., & Fitri, N. (2020). Implementasi dan analisa keamanan jaringan IDS (Intrusion Detection System) menggunakan suricata pada web server. *Jurnal Ilmiah Teknologi Sistem Informasi, 1*(2). doi: 10.30630/jitsi.1.2.10

Yassin, R. M. T. , & Zakaria, A. (2020). 25. Pengembangan skill assesment keamanan jaringan. *Jurnal Teknik*, *18*(2), 123–134. doi: 10.37031/jt.v18i2.78

Yoga, V., & Ardhana, P. (2022). Sistem informasi kebencanaan berbasis android menggunakan metode extreme programming. *Jambura Journal of Informatics*, *4*(2). doi:10.37905/jji.v4i2.16057

Zainuddin, Z. (2021). Tinjauan model pembelajaran blended learning pada perguruan tinggi di era new normal Covid-19: Kebijakan dan implementasi. *Asia-Pacific Journal of Public Policy*, 34–45. doi: 10.52137/apjpp.v7i2.65