BUFNETS
BULLETIN OF NETWORK ENGINEERING AND INFORMATICS
https://bufnets.tech

**BULLETIN OF NETWORK ENGINEERING AND IN*FORM*ATICS**
Vol. 1 No 2 – October 2023

# PENGEMBANGAN SISTEM FIREWALL PADA JARINGAN KOMPUTER BERBASIS MIKROTIK ROUTEROS

## *DEVELOPING A FIREWALL SYSTEM ON A COMPUTER NETWORK BASED ON MIKROTIK ROUTEROS*

**Arief Budi Pratomo**
Laboratorium Komputer dan ICT, STIE Nusa Megarkencana
Kota Yogyakarta, Daerah Istimewa Yogyakarta, Indonesia

e-mail: budiprato@gmail.com

| Received : 06 Mei 2023 | Accepted : 05 Juni 2023 | Published : 1 October 2023 |
|---|---|---|

### *Abstract*

*Network security is crucial in maintaining the confidentiality, integrity, and availability of data. Firewall is one of the important tools to improve computer network security. Mikrotik RouterOS is a popular network operating system that provides a comprehensive firewall feature. However, to optimize the use of the firewall on Mikrotik RouterOS, a more complex firewall system is required. This research aimed to develop a more complex firewall system on a computer network based on Mikrotik RouterOS. The method used is by analyzing the security requirements of the computer network, identifying and analyzing the firewall features available on Mikrotik RouterOS, and designing a more complex firewall system by utilizing these features. The results showed that the developed firewall system can significantly improve computer network security. It includes several firewall configurations such as blocking access to the internet network, blocking access to the local network, bandwidth limitation, and others. Additionally, the firewall system is also equipped with monitoring and logging features to facilitate users in monitoring computer network access. In conclusion, the developed firewall system can enhance the security of a computer network based on Mikrotik RouterOS. This study can contribute to the development of computer network security systems using Mikrotik RouterOS.*

***Keywords:*** *Firewall, Mikrotik RouterOS, Computer Network Security, Firewall Configuration.*

### *Abstrak*

*Keamanan jaringan sangat penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Firewall adalah salah satu alat penting untuk meningkatkan keamanan jaringan komputer. Mikrotik RouterOS adalah sistem operasi jaringan populer yang menyediakan fitur firewall yang lengkap. Namun, untuk mengoptimalkan penggunaan firewall pada Mikrotik RouterOS, diperlukan sistem firewall yang lebih kompleks. Penelitian ini bertujuan untuk mengembangkan sistem firewall yang lebih kompleks pada jaringan komputer berbasis Mikrotik RouterOS. Metode yang digunakan adalah dengan menganalisis kebutuhan keamanan jaringan komputer, mengidentifikasi dan menganalisis fitur firewall yang tersedia pada Mikrotik RouterOS, dan merancang sistem firewall yang lebih kompleks dengan memanfaatkan fitur-fitur tersebut. Hasil penelitian menunjukkan bahwa sistem firewall yang dikembangkan dapat meningkatkan keamanan jaringan komputer secara signifikan. Sistem firewall tersebut terdiri dari beberapa konfigurasi firewall seperti blokir akses ke jaringan internet, blokir akses ke jaringan lokal, pembatasan bandwidth, dan lain sebagainya. Selain itu, sistem firewall juga dilengkapi dengan fitur monitoring dan logging untuk memudahkan pengguna dalam memantau akses jaringan komputer. Kesimpulannya, sistem firewall yang dikembangkan dapat meningkatkan keamanan jaringan komputer berbasis Mikrotik RouterOS. Penelitian ini dapat memberikan kontribusi dalam pengembangan sistem keamanan jaringan komputer menggunakan Mikrotik RouterOS.*

***Kata Kunci:*** *Firewall, Mikrotik RouterOS, Keamanan Jaringan Komputer, Konfigurasi Firewall.*

## 1. PENDAHULUAN

Penggunaan jaringan komputer semakin meningkat seiring dengan perkembangan teknologi informasi yang semakin pesat [1]. Jaringan komputer tidak hanya digunakan untuk kepentingan bisnis, tetapi juga digunakan untuk kepentingan pribadi seperti internet banking dan media social [2]. Namun, semakin banyak penggunaan jaringan komputer, semakin banyak pula ancaman keamanan yang mengintai. Oleh karena itu, keamanan jaringan menjadi suatu hal yang sangat penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data [4].

Firewall merupakan salah satu alat yang efektif untuk meningkatkan keamanan jaringan komputer [5]. Firewall bekerja dengan menghalangi akses ke jaringan komputer yang tidak diizinkan dan membatasi akses yang diperbolehkan [6]. Mikrotik RouterOS adalah salah satu sistem operasi jaringan yang populer dan menyediakan fitur firewall yang lengkap. Fitur firewall pada Mikrotik RouterOS meliputi fitur filter paket, fitur filter konten, fitur filter IP, dan fitur fitur yang lainnya [7].

Namun, untuk mengoptimalkan penggunaan firewall pada Mikrotik RouterOS, diperlukan sistem firewall yang lebih kompleks. Sistem firewall yang kompleks tidak hanya mampu memblokir akses jaringan yang tidak diinginkan, tetapi juga mampu membatasi akses yang diperbolehkan [8]. Sistem firewall yang kompleks juga dapat memantau dan melaporkan akses jaringan secara real-time, sehingga pengguna dapat mengambil tindakan segera apabila terjadi ancaman keamanan [9].

Penelitian ini bertujuan untuk mengembangkan sistem firewall yang lebih kompleks pada jaringan komputer berbasis Mikrotik RouterOS. Penelitian ini akan melibatkan analisis kebutuhan keamanan jaringan, identifikasi dan analisis fitur firewall yang tersedia pada Mikrotik RouterOS, serta rancangan sistem firewall yang lebih kompleks dengan memanfaatkan fitur-fitur tersebut. Selain itu, penelitian ini juga akan mengevaluasi kinerja sistem firewall yang dikembangkan dalam meningkatkan keamanan jaringan.

Hasil penelitian diharapkan dapat memberikan kontribusi dalam pengembangan sistem keamanan jaringan komputer menggunakan Mikrotik RouterOS. Sistem firewall yang dikembangkan akan membantu pengguna jaringan komputer untuk meningkatkan keamanan jaringan yang digunakan. Dengan adanya sistem firewall yang lebih kompleks, pengguna dapat memantau dan melaporkan akses jaringan secara real-time, sehingga dapat mengambil tindakan segera apabila terjadi ancaman keamanan.

## 2. METODE PENELITIAN

Metode penelitian merupakan sebuah cara yang di gunakan sebagai pedoman di dalam melakukan penelitian, sehingga penelitian dapat berjalan dari awal hingga selesai, berikut ini merupakan metode penelitian dari penelitian Pengembangan Sistem Firewall Pada Jaringan Komputer Berbasis MikroTik RouterOS.

a). Studi literatur: Dilakukan untuk mempelajari dasar teori tentang keamanan jaringan komputer, penggunaan firewall, dan fitur-fitur yang tersedia pada Mikrotik RouterOS. Studi literatur juga akan menampilkan tabel berisi penelitian yang memiliki tema yang serupa dengan penelitian ini.

b). Analisis kebutuhan keamanan jaringan: Dilakukan untuk mengidentifikasi kebutuhan keamanan jaringan pada Laboratorium Komputer dan ICT, STIE Nusa Megarkencana, Yogyakarta. Dengan cara mengamati perangkat-perangkat yang harus di amankan.

c). Identifikasi fitur firewall pada Mikrotik RouterOS: Dilakukan untuk mengidentifikasi fitur-fitur firewall yang tersedia pada Mikrotik RouterOS dan mengevaluasi kemampuan fitur-fitur tersebut dalam memenuhi kebutuhan keamanan jaringan yang telah diidentifikasi pada langkah sebelumnya.

d). Rancangan sistem firewall: Dilakukan untuk merancang sistem firewall yang lebih kompleks dengan memanfaatkan fitur-fitur firewall yang tersedia pada Mikrotik RouterOS. Rancangan sistem ini didasarkan pada kebutuhan keamanan jaringan yang telah diidentifikasi pada langkah kedua.

e). Implementasi dan pengujian sistem firewall: Dilakukan untuk mengimplementasikan sistem firewall yang telah dirancang pada langkah sebelumnya. Pengujian sistem dilakukan dengan mensimulasikan serangan keamanan pada jaringan dan mengamati respons sistem firewall terhadap serangan tersebut.

f). Evaluasi kinerja sistem firewall: Dilakukan untuk mengevaluasi kinerja sistem firewall

yang telah dikembangkan dalam meningkatkan keamanan jaringan. Evaluasi ini melibatkan pengukuran waktu respons sistem firewall terhadap serangan keamanan, efektivitas sistem dalam memblokir serangan, dan keterandalan sistem dalam mengidentifikasi ancaman keamanan.

Metode penelitian ini diharapkan dapat memberikan hasil yang akurat dan dapat diandalkan dalam mengembangkan sistem firewall pada jaringan komputer berbasis Mikrotik RouterOS. Dengan melakukan studi literatur, analisis kebutuhan keamanan jaringan, identifikasi fitur firewall, rancangan sistem firewall, implementasi dan pengujian, serta evaluasi kinerja sistem firewall, diharapkan sistem firewall yang dikembangkan dapat meningkatkan keamanan jaringan secara signifikan.

## 3. HASIL DAN PEMBAHASAN

### 3.1 Studi Literatur

Studi literatur dalam penelitian pengembangan sistem firewall pada jaringan komputer berbasis Mikrotik RouterOS dilakukan untuk memperoleh pemahaman yang lebih baik tentang keamanan jaringan komputer, penggunaan firewall, dan fitur-fitur yang tersedia pada Mikrotik RouterOS.
Studi literatur juga dilakukan untuk mengidentifikasi kekurangan dan kelebihan fitur firewall pada Mikrotik RouterOS.

Berikut ini tabel 1 yang memuat beberapa penelitian sebelumnya yang memiliki tema yang sama serta menjelaskan perbedaan penelitian tersebut dengan penelitian yang dilakukan.

Tabel 1: Penelitian sebelumnya dengan tema yang sama

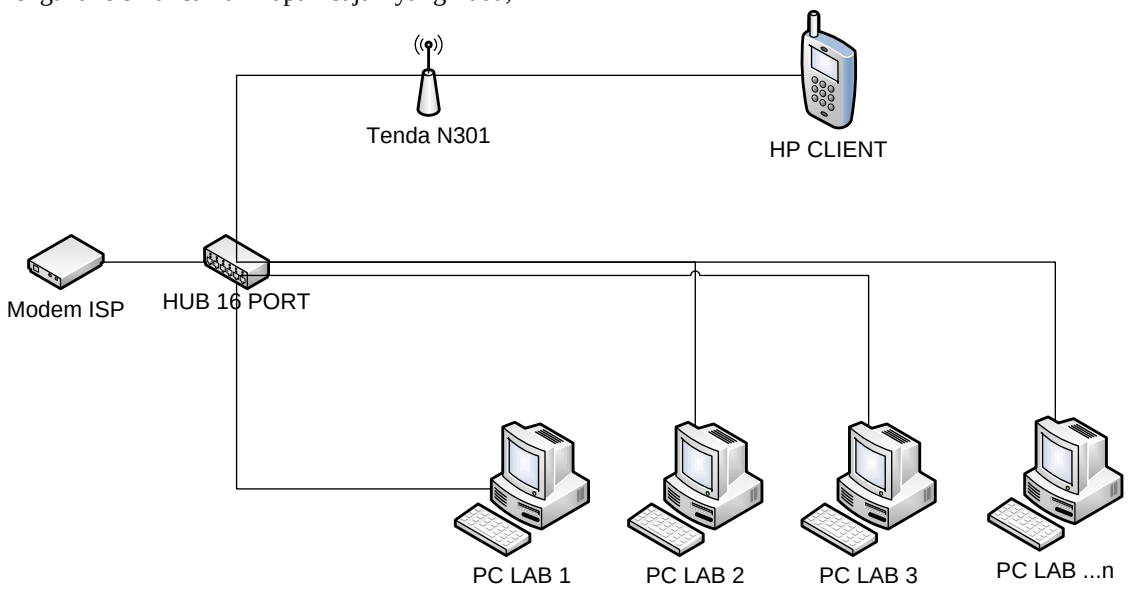
| No | Judul | Penulis | Keterangan |
|---|---|---|---|
| **1** | Implementasi Cloud Computing Sebagai Radius Server Pada Jaringan Internet Router Mikrotik | Saputra, I. P., Yusuf, R., & Saprudin, U. (2021). | Penelitian sebelumnya menekankan penelitianya untuk membandingkan antara infrastruktur cloud dan tradisional, namun dapat di tarik kesimpulan tentang pemanfaatan fitur hotspot pada mikrotik yang dapat digunakan untuk memanajemen pengguna hotspot [7]. |
| **2** | Manajemen Bandwidth Menggunakan Metode Queue Tree dan Keamanan Hotspot Menggunakan Mikrotik Os dan Gns3di Balai Desa Sidorejo | Hakim, R. P. N. M., Raharjo, S., & Kusumaningsih, R. Y. R. (2021). | Penelitian ini bertujuan untuk meningkatkan keandalan sebuah jaringan internet dengan memanajemen bandwidth yang ada, dengan manajemen bandwidth yang baik koneksi internet menjadi stabil dan lancar [10]. |
| **3** | *Analysis Of Vulnerabilityassessment With Penetration Testing* | Mohan, A., & Swaminathan, D. G. A. (2022). | Penelitian ini bertujuan untuk menemukan beberapa kelemahan yang ada pada sebuah instansi dengan melakukan scanning vulnerability, hasilnya terdapat beberapa kelemahan yang ditemukan, hal ini menginspirasi untuk melakukan scanning vulnerability pada Laboratorium Komputer dan ICT, STIE Nusa Megarkencana, Yogyakarta. untuk menemukan kelemahan yang ada dan memperbaiki kelemahan tersebut [11]. |
| **4** | Analisa dan Problem Solving Keamanan Router Mikrotik Rb750ra Dan Rb750g R3 Dengan Metode Penetration Testing (Studi Kasus: Warnet Aulia.Net, Tanjung Harapan Lampung Timur) | Hidayat, A., & Saputra, I. P. (2018). | Penelitian ini berfokus di dalam mendeteksi kelemahan yang ada pada perangkat jaringan, setiap perangkat yang ada pada jaringan dengan sistem operasi yang beragam, dapat memiliki celah keamanan yang dapat di eksploitasi oleh bad actors [12]. |

Beberapa penelitian yang terdapat pada tabel 1 merupakan beberapa penelitian yang dapat dijadikan rujukan di dalam membangun sistem firewall guna mengamankan jaringan komputer yang ada pada Laboratorium Komputer dan ICT, STIE Nusa Megarkencana, Yogyakarta.

### 3.2 Analisis Kebutuhan

Dalam menganalisis kebutuhan diperlukan menganalisis ancaman apa saja yang ada, ancaman dapat di lihat dengan melakukan proses analisis perangkat yang ada, sistem operasi yang digunakan dan aplikasi apa saja yang akan digunakan.

Berikut ini Gambar 1 yang merupakan topologi dari jaringan komputer yang ada pada Laboratorium Komputer dan ICT, STIE Nusa Megarkencana, Yogyakarta.




Gambar 1. Topologi Jaringan Laboratorium Komputer dan ICT, STIE Nusa Megarkencana, Yogyakarta
[Sumber: Penulis, 2023]

Dari Gambar 1 dapat di jelaskan bahwa terdapat beberapa perangkat yang ada pada jaringan komputer Laboratorium Komputer dan ICT, STIE Nusa Megarkencana, Yogyakarta. Perangkat-perangkat tersebut memiliki kerentanan terhadap serangan cyber berbasis jaringan. Pada Gambar 1 memperlihatkan tidak adanya firewall yang terpasang pada jaringan yang dapat menjadi penangkal serangan pada jaringan, selain itu beberapa kelemahan yang ada pada jaringan dapat dijelaskan pada Tabel 2.

Berikut ini Tabel 2 yang merupakan hasil dari analisis kebutuhan pada Laboratorium Komputer dan ICT, STIE Nusa Megarkencana, Yogyakarta.

Tabel 2: Hasil analisis kebutuhan

| No | Kelemahan | Kebutuhan |
|---|---|---|
| **1** | Tidak adanya firewall yang digunakan untuk mengatur dan memfilter jaringan komputer LAB dari serangan. | Di butuhkan perangkat MikroTik yang dapat memfilter konten yang dapat mengganggu keamanan jaringan. |
| **2** | PC pada laboratoirum menggunakan sistem operasi windows yang membuka port-port tertentu | Memblokir akses port yang tidak digunakan |
| **3** | Akses point tenda yang digunakan tidak menggunakan password autentikasi | Memanfaatkan fitur hotspot pada RouterOS MikroTik |
| **4** | Tidak adanya manajemen bandwidth | Memanfaatkan fitur manajemen pada RouterOS MikroTik |

Dari hasil analisis kebutuhan yang ada pada Tabel 2, RouterOS MikroTik dapat menjadi solusi dari kelemahan yang telah ditemukan, dengan ditemukanya masalah tersebut kita dapat memilah fitur-fitur yang ada pada router MikroTik untuk mengatasi kelemahan yang ada pada jaringan komputer Laboratorium Komputer dan ICT, STIE Nusa Megarkencana, Yogyakarta.

### 3.3 Identifikasi fitur firewall pada Mikrotik RouterOS

Pada tahap analisis kebutuhan, dibutuhkan beberapa langkah di dalam mengamankan jaringan yang ada pada Laboratorium Komputer dan ICT, STIE Nusa Megarkencana, Yogyakarta. Pada tabel 2 terdapat kolom kelemahan yang merupakan celah yang ada pada masing-masing perangkat yang ada pada jaringan. Untuk itu beberapa fitur firewall yang ada pada Router MikroTik akan digunakan untuk menangkal kelemahan yang ada pada jaringan komputer Laboratorium Komputer dan ICT, STIE Nusa Megarkencana, Yogyakarta.

Berikut ini Tabel 3 yang berisi fitur dari Routeros MikroTik yang akan digunakan untuk mengatasi kelemahan yang ditemukan.

Tabel 3: Fitur RouterOS MikroTik

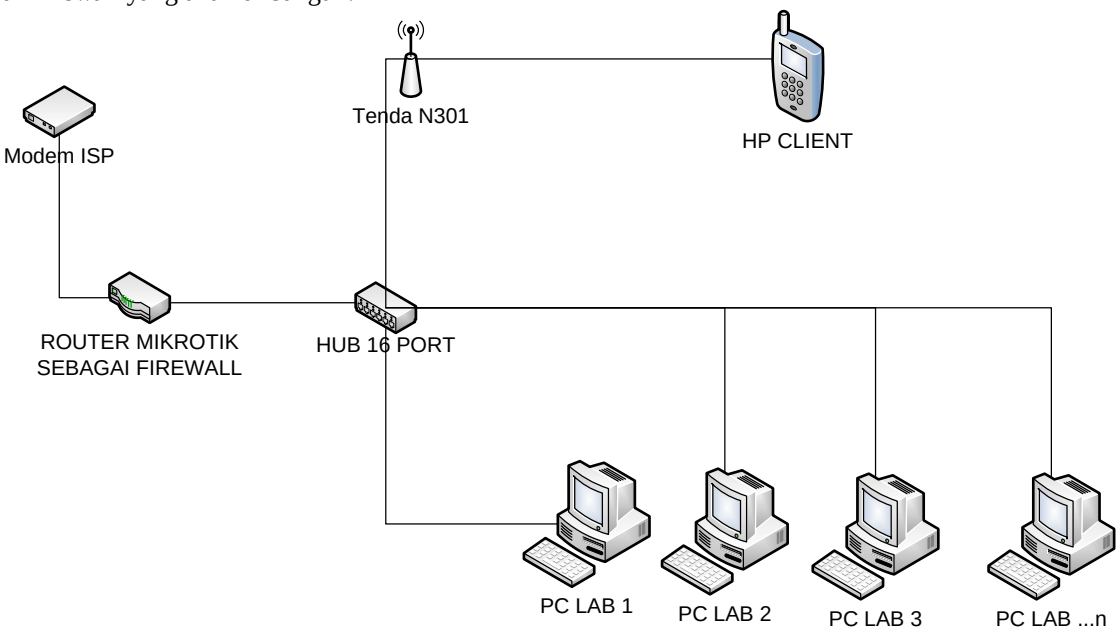
| No | Fitur | Keterangan |
|---|---|---|
| **1** | Filter Rules | Filter rules pada MikroTik adalah aturan-aturan yang digunakan untuk mengatur lalu lintas data di jaringan, dengan beberapa kriteria seperti protocol, address, port, action, time, interface, dan connection state, sehingga administrator jaringan dapat mengatur lalu lintas data dengan lebih tepat dan efektif, memastikan keamanan dan kinerja jaringan yang optimal [13]. |
| **2** | NAT | Network Address Translation (NAT) adalah fitur pada MikroTik yang berfungsi untuk mengubah alamat IP asal dan tujuan paket data yang melewati router, sehingga dapat menambah keamanan jaringan dengan menyembunyikan alamat IP asli jaringan lokal [14]. NAT juga memungkinkan penggunaan satu alamat IP publik untuk banyak perangkat di jaringan lokal dan membantu mengoptimalkan penggunaan koneksi internet [15]. Dengan menggunakan NAT, administrator jaringan dapat meningkatkan keamanan jaringan dan efisiensi penggunaan sumber daya jaringan. |
| **3** | Mangle | Mangle pada MikroTik adalah fitur yang digunakan untuk memodifikasi paket data saat melewati router [16]. Fitur ini memungkinkan administrator jaringan untuk melakukan manipulasi pada header paket data, seperti mengubah nilai tos, mengganti port sumber atau tujuan, dan melakukan marking pada paket data, sehingga dapat memudahkan dalam manajemen lalu lintas jaringan dan meningkatkan keamanan jaringan. Mangle biasanya digunakan untuk mengatur QoS (Quality of Service), routing, dan firewall pada jaringan, serta dapat membantu meningkatkan performa dan efisiensi jaringan [17]. |
| **4** | Address List | Fitur ini juga dapat digunakan untuk mempermudah proses konfigurasi pada fitur-fitur lainnya di MikroTik seperti Firewall, NAT, Mangle, dan lainnya. Address List juga dapat di-update secara otomatis melalui fitur Dynamic Address List yang memungkinkan pengguna untuk menambahkan alamat IP yang tidak diketahui sebelumnya ke dalam daftar secara otomatis. Dengan menggunakan Address List, administrator jaringan dapat mengelola alamat IP dengan lebih mudah dan efektif, meningkatkan keamanan dan kinerja jaringan [18]. |
| **5** | Layer 7 Protocols | Layer 7 Protocol memungkinkan administrator jaringan untuk memantau dan mengontrol lalu lintas jaringan berdasarkan jenis aplikasi atau protokol yang digunakan. Dengan mengidentifikasi dan membatasi penggunaan Layer 7 Protocol tertentu, administrator jaringan dapat meningkatkan keamanan, kinerja, dan efisiensi jaringan secara keseluruhan [19]. |
| **6** | Queues | Queues pada MikroTik adalah fitur yang digunakan untuk mengatur bandwidth dan prioritas lalu lintas jaringan. Queues memungkinkan administrator jaringan untuk mengontrol kecepatan dan penggunaan bandwidth jaringan, serta memprioritaskan lalu lintas jaringan berdasarkan jenis aplikasi atau protokol yang digunakan [20]. |
| **7** | Hotspot | Fitur hotspot pada MikroTik dilengkapi dengan berbagai fitur keamanan dan manajemen pengguna, seperti autentikasi pengguna, manajemen bandwidth, dan kontrol akses berbasis waktu. Hal ini memungkinkan administrator jaringan untuk mengelola dan membatasi akses pengguna ke jaringan WiFi dan internet, |

| | | |
|---|---|---|
| | | serta mengumpulkan data dan informasi pengguna untuk analisis lebih lanjut [7]. |

### 3.4 Rancangan sistem firewall

Dalam perancangan sistem firewall diperlukan topologi, untuk menggambarkan sistem kerja dari firewall yang akan di bangun.

Berikut ini Gambar 1 merupakan topologi dari sistem firewall yang akan di bangun.



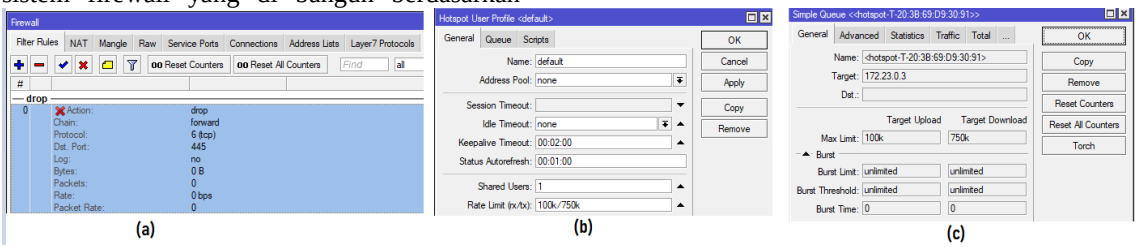

Gambar 2. Rancangan Firewall, Laboratorium Komputer dan ICT, STIE Nusa Megarkencana, Yogyakarta
[Sumber: Penulis, 2023]

Terdapat perbedaan antara Gambar 2 dan Gambar 1, dimana pada Gambar 2, terdapat perangakat Routerboard MikroTik yang dapat dimanfaatkan sebagai firewall yang dapat melindungi perangkat yang ada pada jaringan komputer [7].

### 3.5 Implementasi dan pengujian sistem firewall

Tahapan ini adalah tahap mengimplementasikan dan menguji sistem firewall yang di bangun, sistem firewall yang di bangun berdasarkan kebutuhan dan kelemahan yang ada pada jaringan, kebutuhan dan kelemahan yang ditemukan pada tahap sebelumnya dapat di atasi dengan beberapa konfigurasi dan aturan firewall yang dibuat menggunakan MikroTik RouterOS.

Berikut merupakan Gambar 3 yang berisi beberapa aturan firewall dan konfigurasi yang dibuat pada MikroTik RB450 Laboratorium Komputer
dan ICT, STIE Nusa Megarkencana, Yogyakarta.




Gambar 3. Konfigurasi dan rule firewall Mikrotik RouterOS
[Sumber: Penulis, 2023]

Penjelasan gambar 3:

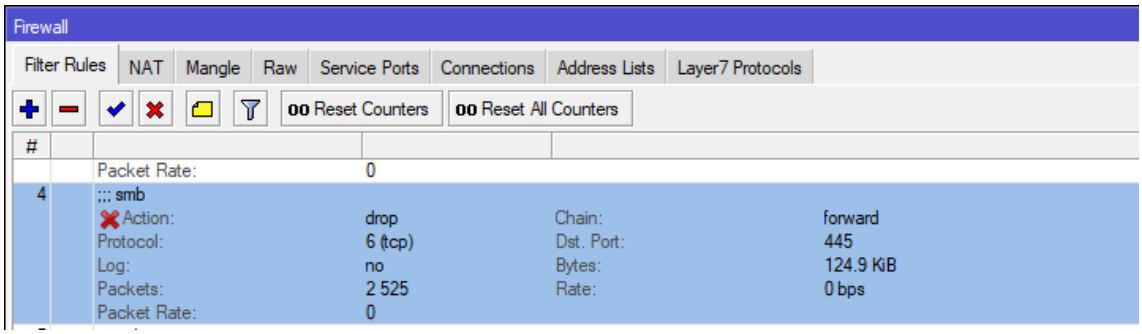
a). Blokir port 445: untuk mencegah penggunaan *port* 445 yaitu port yang digunakan untuk service *SMB* dan *Microsoft active directory* [21]. Port 445 tidak di gunakan pada LAB dan memiliki celah keamanan salah satunya adalah *Remote Code Execution* [22],[23], untuk itu port tersebut perlu di blokir menggunakan rule firewall MikroTik.

b). konfigurasi user profil hotspot: ini digunakan untuk mengautentikasi pengguna, sebelum pengguna menggunakan jaringan komputer.

c). Simple queue: pengguna yang telah melewati proses autentikasi akan otomatis di batasi kecepatan internetnya, hal ini bertujuan untu mencegah monopoli bandwidth oleh pengguna [7].

### 3.6 Evaluasi kinerja sistem firewall

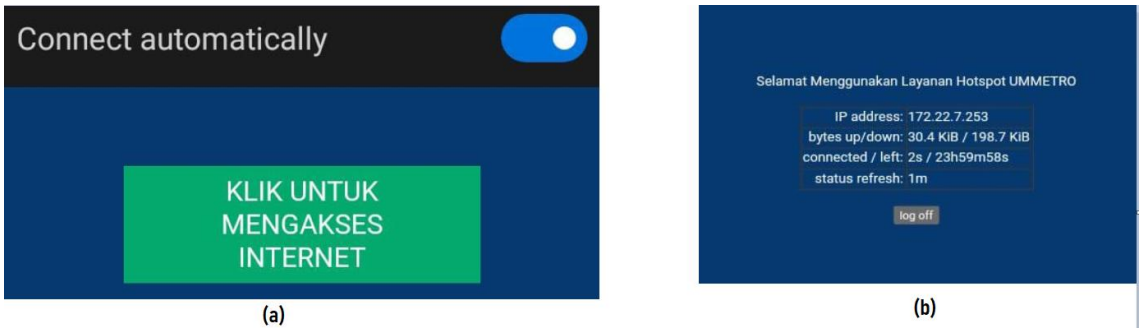
Dari proses implementasi dan pengujian, beberapa temuan dari ujicoba tersebut akan menghasilkan kesimpulan dari penelitian. Pada tahap uji coba serangan, penulis menguji untuk menggunakan port 445 pada jaringan dan melihat apakah router mampu mendeteksi dan memblokir serangan tersebut. Berikut ini Gambar 4 yang menunjukan bahwa firewall rule telah berhasil mendeteksi serangan.




Gambar 4. Firewall rule mendeteksi dan memblokir port 445
[Sumber: Penulis, 2023]

Gambar 4 menunjukan bahwa router memblokir akses port 445 yang melewati router, aksi ini akan mengentikan PC client yang melakukan sharing data maupun sharing printer [24], namun hal tersebut tidak bermasalah, sebab LAB tidak digunakan untuk kegiatan tersebut.

Setelah melakukan ujicoba menggunakan port 445, penulis melakukan ujicoba penggunaan jaringan komputer, hal ini dilakukan untuk menguji apakah hotspot telah berhasil di lakukan. Berikut ini Gambar 5 yang menunjukan proses autentikasi hotspot.




Gambar 5. Proses autentikasi hotspot
[Sumber: Penulis, 2023]

Hotspot yang di konfigurasi, menggunakan mode trial, dimana mode ini tidak memerlukan username dan password, proses autentikasi akan mencatat mac-address pengguna dan membatasi kecepatan (bandwith) dari pengguna.

Berikut ini Tabel 4 yang berisi proses uji coba speedtest yang dilakukan menggunakan perangkat jaringan yang terhubung dengan jaringan LAB.

Tabel 4: Ujicoba pembagianbandwidth

| No | DEVICE | Rata-rata Download Speed (kbps) | Rata-rata Upload Speed (kbps) |
|---|---|---|---|
| **1** | Device 1 | 732 | 97 |
| **2** | Device 2 | 706 | 89 |
| **3** | Device 3 | 718 | 96 |

| | | | |
|---|---|---|---|
| **4** | Device 4 | 700 | 95 |
| **5** | Device 5 | 728 | 98 |
| **6** | Device 6 | 720 | 92 |
| **7** | Device 7 | 714 | 94 |
| **8** | Device 8 | 721 | 97 |
| **9** | Device 9 | 722 | 93 |
| **10** | Device 10 | 726 | 96 |

Proses ujicoba dilakukan sebanyak 5 kali percobaan, proses ujicoba dilakukan dengan cara device 1 sampai device 10 melakukan ujicoba speedtest secara bersamaan, tabel 4 menunjukan dari device 1 sampai device 10 mendapatkan hasil rata-rata yang hampir sama dan merata. Hal ini menunjukan bahwa proses pembagian bandwidth telah berhasil dapat mencegah monopoli bandwidth [25].

## 4. KESIMPULAN

Berdasarkan penelitian, analisis dan pembahasan pada penelitian ini, maka dapat diambil kesimpulan sebagai berikut :

1. Implementasi firewall pada jaringan LAB berhasil dalam mendeteksi dan memblokir serangan yang mencoba menggunakan port 445.
2. Selain itu, hotspot juga telah berhasil diimplementasikan dengan sukses melalui proses autentikasi.
3. Ujicoba speedtest juga menunjukan bahwa pembagian bandwidth telah berhasil dilakukan dengan baik, mencegah terjadinya monopoli bandwidth.

Oleh karena itu, dapat dikatakan bahwa implementasi firewall dan hotspot pada jaringan LAB telah berhasil meningkatkan keamanan dan pengaturan bandwidth pada jaringan tersebut.

## PERNYATAAN PENGHARGAAN

Kepada seluruh tim di Laboratorium Komputer dan ICT, STIE Nusa Megarkencana Kota Yogyakarta, saya ingin mengucapkan terima kasih atas kesempatan dan kepercayaan yang diberikan untuk melakukan pengembangan sistem firewall pada jaringan komputer berbasis Mikrotik RouterOS di laboratorium tersebut. Saya berharap hasil dari pengembangan ini dapat memberikan manfaat dan meningkatkan keamanan jaringan komputer di laboratorium tersebut. Terima kasih juga kepada seluruh tim yang telah bekerja sama dalam proses pengembangan ini. Semoga kerja sama kita dapat terus berlanjut di masa depan.

## DAFTAR PUSTAKA

[1] Febriansyah, F. I., Indiantoro, A., & Ikhwan, A. (2023). MODEL KEJAHATAN DUNIA MAYA (CYBERCRIME) SEBAGAI UPAYA PEMBENTUKAN HUKUM NASIONAL. Legal Standing: Jurnal Ilmu Hukum, 7(2), 183-196.

[2] Nurmansyah, G. PERLINDUNGAN HUKUM BAGI KORBAN CYBERCRIME DATA FORGERY PADA SEKTOR PERBANKAN MELALUI INTERNET (E-BANKING). PERDATA, 1(3), 96.

[3] Syafrial, H. (2023). Literasi Digital Seri 1. Nas Media Pustaka.

[4] Saputra, I. P., Utami, E., & Muhammad, A. H. (2022, October). Comparison of anomaly based and signature based methods in detection of scanning vulnerability. In 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 221-225). IEEE.

[5] Pratama, C. M. I. OPTIMALISASI KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN METODE KNOCKING PORT BERBASIS MIKROTIK.

[6] Hidayat, A. (2023). ABNORMAL TRAFFIC ANALYSIS USING WIRESHARK (CASE STUDY: SISTER.UMMETRO.AC.ID). BULLETIN of NETWORK ENGINEER and INFORMATICS, 1(1), 7–11. https://bufnets.tech/index.php/bufnets/article/view/4/10

[7] Saputra, I. P., Yusuf, R., & Saprudin, U. (2021). IMPLEMENTASI CLOUD COMPUTING SEBAGAI RADIUS SERVER PADA JARINGAN INTERNET ROUTER MIKROTIK. Journal Computer Science and Information Systems: J-Cosys, 1(2), 81-86.

[8] KURNIAWAN, I. A. (2022). ANALISA JARINGAN RT/RW NET SEBAGAI HOTSPOT PELAJAR (Studi Kasus RT 01&02 RW 08 Sumberrejo, Pandansari)

(Doctoral dissertation, UNIVERSITAS MUHAMMADIYAH MAGELANG).

[9] Fernandes, J. (2022). Analisis Keamanan Jaringan Wireles LAN Di Dinas Perpustakan Dan Kearsipan Kota Pekanbaru (Doctoral dissertation, Universitas Islam Riau).

[10] Hakim, R. P. N. M., Raharjo, S., & Kusumaningsih, R. Y. R. (2021). MANAJEMEN BANDWIDTH MENGGUNAKAN METODE QUEUE TREE DAN KEAMANAN HOTSPOT MENGGUNAKAN MIKROTIK OS DAN GNS3 DI BALAI DESA SIDOREJO. Jurnal Jarkom, 9(1), 63-70.

[11] Mohan, A., & Swaminathan, D. G. A. (2022). Analysis of Vulnerabilityassessment with Penetration Testing. Available at SSRN 4040684.

[12] Hidayat, A., & Saputra, I. P. (2018). Analisa Dan Problem Solving Keamanan Router Mikrotik Rb750Ra Dan Rb750Gr3 Dengan Metode Penetration Testing (Studi Kasus: Warnet Aulia. Net, Tanjung Harapan Lampung Timur). Jurnal RESISTOR (Rekayasa Sistem Komputer), 1(2), 118-124.

[13] Novianto, D., Japriadi, Y. S., & Tommy, L. (2023). Optimalisasi Koneksi Local Area Network (LAN) Menggunakan Metode Fasttrack Pada Routerboard Mikrotik. JURNAL MEDIA INFOTAMA, 19(1), 224-229.

[14] Ardianto, F., Alfaresi, B., & Darmadi, A. (2018). Rancang Bangun Load Balancing Dua Internet Service Provider (ISP) Berbasis Mikrotik. Jurnal Surya Energy, 3(1), 198-202.

[15] Malik, A. N. (2023). LKP: Simulasi Desain Load Balancing dengan Menggunakan Metode NTH (Doctoral dissertation, Universitas Dinamika).

[16] Rahman, T., Ibrahim, B., Nurdin, H., & Qomaruddin, M. (2023). HIERARCHICAL TOKEN BUCKET (HTB) PADA QUALITY OF SERVICE PT. EKA BOGAINTI. Rabit: Jurnal Teknologi dan Sistem Informasi Univrab, 8(1), 82-91.

[17] Muslim, I. (2023). PERANCANGAN DAN IMPLEMENTASI VPN SEBAGAI QoS GAME ONLINE PADA JARINGAN BERBASIS MIKROTIK (Doctoral dissertation, Institut Teknologi Nasional Malang).

[18] 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. Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi), 13(1).

[19] Tahir, M., & Kom, M. T. (2023). PENGANTAR JARINGAN KOMPUTER DASAR. CV Literasi Nusantara Abadi.

[20] Noviansyah, M. (2023). EFISIENSI JARINGAN KOMPUTER DENGAN PENERAPAN FIREWALL MANGLE DAN BANDWIDTH LIMIT DENGAN METODE PER CONNECTION QUEUING (PCQ). Akrab Juara: Jurnal Ilmu-ilmu Sosial, 8(1).

[21] Priya, V. D., & Chakkaravarthy, S. S. (2023). Containerized cloud-based honeypot deception for tracking attackers. Scientific Reports, 13(1), 1437.

[22] sleepya. (2017, July 11). Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - “EternalBlue” SMB Remote Code Execution (MS17-010). Exploit Database. https://www.exploit-db.com/exploits/42315

[23] Microsoft. (2017, March 14). Microsoft Security Bulletin MS17-010 - Critical. Learn.microsoft.com. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

[24] Alliance, C. C. I. (2023). Review of Cyberattacks from US Intelligence Agencies.

[25] Gustiawan, M., Yudianto, R. J., Pratama, J., & Fauzi, A. (2021). Implementasi Jaringan Hotspot Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer. Jurnal Nasional Komputasi dan Teknologi Informasi, 4(4), 244-247.