

IMPLEMENTASI KEAMANAN JARINGAN DENGAN METODE *FIREWALL FILTERING* MENGGUNAKAN *MIKROTIK* DI SMKN 3 PAYAKUMBUH

Khairul Aziz, Supratman zakir, Wedra Aprison, Liza Efriyanti

Teknik Informatika dan Komputer, Universitas Islam Negeri Sjech M.Djamil Djambek Bukittinggi.
Khairulaziz281100@gmail.com

ABSTRAK

Tujuan dari penelitian ini adalah keamanan jaringan dengan metode *firewall filtering* menggunakan *mikrotik router RB941* di SMKN 3 Payakumbuh sering terjadinya keluhan guru tentang jaringan yang membuat para siswa tidak fokus untuk melakukan pembelajaran di kelas serta membuka berbagai situs website, game ONLINE dst. Berdasarkan hal tersebut maka dibutuhkan keamanan jaringan dengan metode *firewall filtering* menggunakan *mikrotik router* di SMKN 3 Payakumbuh agar pengguna jaringan menjadi fokus dalam hal pembelajaran. Penelitian keamanan jaringan dengan metode *firewall filtering* menggunakan *mikrotik* di SMKN 3 Payakumbuh menggunakan metode penelitian *Research and Development (R&D)* dengan model pengembangan PPDIIO (*Prepare, Plan, Design, Implement, Operate, Optimize*). Uji produk dalam penelitian ini adalah uji validitas, uji praktikalitas serta uji efektivitas. Pada sistem ini keamanan jaringan dengan metode *firewall filtering* menggunakan Layer 7 Protocol, IP address serta IP Komputer untuk memutuskan suatu jaringan memblock suatu situs website, sosial media atau game online. Hasil penelitian menunjukkan bahwa *mikrotik router* berhasil memblock situs website, media sosial atau game online. Metode *firewall filtering* menggunakan *mikrotik* dapat memenuhi kebutuhan sistem, sehingga keamanan jaringan dengan metode *firewall filtering* menggunakan *mikrotik router* tidak dapat diakses oleh siswa atau pengguna jaringan sesuai dengan ketentuan yang telah dirancang sebelumnya.

Kata kunci : *Firewall Filtering, Mikrotik*

1. PENDAHULUAN

Kemajuan telekomunikasi pula amat diperlukan dalam pendidikan hingga itu di tiap sekolah diwajibkan memiliki jaringan internet buat aktivitas berlatih membimbing. Tetapi di bagian lain jaringan internet dapat berakibat minus dikala di akses sebab banyak web yang beraroma berusia tanpa terdapat pengawasan spesial. Dalam aspek ilmu komputer, ada banyak tata cara yang dibesarkan dengan tata cara lain, tercantum perkembangan teknologi di dalam keamanan jaringan. Salah satu keamanan jaringan memakai *mikrotik Router* ataupun *Cisco Router*. Sebagian riset mengenai keamanan jaringan sudah dicoba lebih dahulu, ialah oleh Alfin Hikmaturokhman, Adnan Purwanto, Rendy Munadi (2010) yang bertajuk “Analisa Penyusunan Serta Aplikasi Firewall Serta Traffic Filtering Memakai *Cisco Router*” Bagi hasil kajian, periset hendak membuat suatu sistem keamanan jaringan buat menolong penanganan permasalahan biar diperoleh layanan nyaman serta maksimum. Dengan tata cara Firewall Serta Traffic Filtering Memakai *Mikrotik Router*”.

Firewall bisa dimaksud selaku sesuatu bagian yang bisa menghalangi akses dampingi jaringan yang dilindungi, firewall bisa jadi pemecahan buat menanggulangi keamanan dalam sesuatu jaringan yang bisa dipadati dengan bermacam bahaya bagus di dalam ataupun di luar jaringan. Dengan bentuk yang betul, ini membolehkan buat mencegah kemudian rute. Kemudian rute ataupun kemudian rute dapat lebih bagus serta lebih aman[1].

Pada hasil wawancara dengan sebagian guru di Sekolah Menengah Kejuruan(SMK) Negara 3 Payakumbuh, didapat sebagian data kalau anak didik kala dalam cara penataran memakai jaringan internet, kerap menyalahgunakan jaringan semacam membuka permainan, youtube, facebook, intagram serta lain-lain. Oleh sebab itu anak didik tidak fokus pada penataran.

Perihal ini menimbulkan pemakaian internet dalam cara penataran yang membuat anak didik tidak bisa maksimal dalam cara penataran yang berhubungan dengan jaringan internet. Riset ini bermaksud Buat memperoleh hasil yang cocok dengan impian.

Bersumber pada kerangka balik permasalahan ini hingga pengarang melaksanakan riset yang bertajuk, Implementasi Keamanan Jaringan Dengan Metode *Firewall Filtering* Menggunakan *Mikrotik* Di SMK Negeri 3 Payakumbuh.

2. TINJAUAN PUSTAKA

2.1. Jaringan

a. Konsep dasar jaringan komputer

Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan anatara komputer dengan komputer lainnya yang saling berhubungan dan saling bertukar data. Tujuan dari jaringan komputer adalah agar bisa mencapai tujuannya, pada bagian di setiap komputer bisa memberikan seerta meminta layanan (*service*). Pihak menerima atau meminta layanan disebut dengan klien (*client*) serta yang melakukan pengiriman atau yang memberrikan layanan disebut dengan peladen

(server). Desain tersebut bernama sistem *client-server*, serta dipakai pada hampir semua aplikasi jaringan komputer[1].

Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan satu dengan yang lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, aplikasi dan perangkat keras secara bersama-sama. Jaringan komputer dapat diartikan juga sebagai kumpulan sejumlah terminal komunikasi yang berada di berbagai lokasi yang terdiri dari lebih dari satu komputer yang saling berhubungan. Jaringan komputer pada umumnya adalah hubungan banyak komputer ke satu atau beberapa server. Server adalah komputer yang berfungsi sebagai “pelayan” pengiriman data atau penerimaan data serta mengatur pengiriman dan penerimaan data di antara komputer-komputer yang tersambung.

b. Pengertian keamanan jaringan

Keamanan jaringan adalah proses terjadinya pencegahan dan mengidentifikasi kepada pengguna yang tidak sah, atau penggunaan secara ilegal dari komputer ke jaringan[2].

c. Tujuan keamanan jaringan

Tujuannya adalah untuk mengantisipasi resiko jaringan komputer yang dapat berupa ancaman fisik maupun *logic*. Yang dimaksud ancaman fisik adalah yang merusak bagian fisik komputer atau *hardware* komputer sedangkan ancaman logik yaitu berupa pencuriandata atau penyusup yang membobol akun seseorang [3].

2.2. Keamanan Jaringan

a. Pengertian keamanan jaringan

Keamanan jaringan adalah proses terjadinya pencegahan dan mengidentifikasi kepada pengguna yang tidak sah, atau penggunaan secara ilegal dari komputer ke jaringan[2].

b. Tujuan keamanan jaringan

Tujuannya adalah untuk mengantisipasi resiko jaringan komputer yang dapat berupa ancaman fisik maupun *logic*. Yang dimaksud ancaman fisik adalah yang merusak bagian fisik komputer atau *hardware* komputer sedangkan ancaman logik yaitu berupa pencuriandata atau penyusup yang membobol akun seseorang [3].

c. Confidentiality

Sistem harus memastikan bahwa informasi dikomunikasi dan disimpan secara aman dan hanya dapat diakses oleh mereka yang berhak saja. Data-data pribadi yang bersifat pribadi harus dapat terjaga dan dapat dipastikan terproteksi dengan baik [4].

d. Integrity

Aspek ini harus mengutamakan data atau informasi tidak boleh diakses tanpa seizin pemiliknya [5].

e. Authenticity

Sistem harus memastikan bahwa pihak, objek dan informasi yang berkomunikasi adalah riil dan bukan palsu. Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking (untuk menjaga “intellectual property”, yaitu dengan menilai dokumen atau hasil karya dengan “tangan” pembuat) dan digital *signature*. Metode *authenticity* yang paling umum digunakan adalah penggunaan *username* beserta *password*nya [4].

f. Availability

Dalam aspek ini berkaitan dengan apakah ada suatu data yang tersedia Ketika dibutuhkan atau diperlukan oleh pengguna. Jika sebuah data atau informasi sangat ketat dalam pengamanannya maka dapat menyulitkan dalam mengakses data tersebut. Dan juga akses yang lambat dapat juga menghambat aspek *availability* [6].

2.3. Firewall

Firewall merupakan suatu fitur ataupun sistem yang digunakan untuk memfilter paket data dari luar ataupun dari dalam jaringan yang tersambung dalam satu jaringan. *Firewall* merupakan alat yang digunakan untuk menghindari orang luar untuk mendapatkan akses ke suatu jaringan komputer. *Firewall* tersebut berperan untuk mengizinkan lalu lintas jaringan yang dianggap aman untuk melalui serta menghindari lalu lintas yang dianggap tidak aman. Umumnya, sebuah *Firewall* diterapkan dalam sebuah mesin terdeteksi yang berjalan pada pintu gerbang antara jaringan local serta jaringan yang lain. *Firewall* hendak melaksanakan monitoring terhadap seluruh paket data jaringan yang melewatinya serta paket data yang dianggap tidak aman atau serangan akan tersimpan didalam file yang dinamakan log yang berada pada *firewall* [7].

Fungsi *firewall* adalah sebagai pengontrol, mengawasi suatu arus paket data yang mengalir pada jaringan. Fungsi *firewall* yaitu mengatur, menyaring dan mengontrol lalu lintas data yang sudah diizinkan untuk mengakses jaringan *privat* yang dilindungi, beberapa kriteria yang dilakukan *firewall* apakah dapat memperoleh paket data lewat atau tidak[8].

- Alamat IP dari komputer sumber.
- Port TCP/UDP sumber dari sumber.
- Alamat IP dari komputer tujuan.
- Port TCP/UDP tujuan data pada komputer tujuan.

2.4. Web Filtering

Cara kerja dari web *filtering* ini yaitu dapat memblokir akses web yang dianggap mengandung konten yang tidak pantas. Jadi menyediakan beberapa fitur dengan beberapa cara atau teknik. Fitur atau *policy* dapat memblokir web yang dapat di terapkan pada *mikrotik* diantaranya yaitu DNS, *web proxy*, *router policy*, *content filter*, *layer 7 firewall* dan *destination IP address/port block* [9].

2.5. Winbox

Winbox adalah sebuah utility yang dapat digunakan untuk melakukan remote ke server mikrotik dalam mode GUI. Jika untuk mengkonfigurasi mikrotik dalam text mode melalui PC itu sendiri, maka untuk GUI yang menggunakan winbox kita perlu mengkonfigurasi mikrotik melalui komputer Clint. Mengkonfigurasi mikrotik melalui winbox ini lebih banyak digunakan karena selain penggunaannya yang mudah, juga tidak harus menghafal perintah-perintah consule [10].

2.6. Mikrotik

a. Pengertian Mikrotik

Mikrotik routerOS adalah sistem operasi linux base yang diperuntukkan sebagai network router. Desain untuk memberikan kemudahan bagi pengguna. Administrasi bisa dilakukan melalui windows application (winbox) berhubungan dengan sistem jaringan komputer. Mikrotik adalah sebuah sistem operasi termasuk didalamnya perangkat lunak yang dipasang pada suatu komputer sehinggalah komputer tersebut dapat berperan sebagai inti network, pengendalian dan pengecualian lalu lintas data antara jaringan, komputer ini disebut sebagai router [11].

Kemampuan Mikrotik dapat disejajarkan dengan router kelas enterprise dengan harga yang jauh lebih murah. Hal ini menjadi relevan bila dilihat Sebagian besar pengguna Mikrotik berasal dari negara berkembang[9].

b. Jenis-jenis Mikrotik

- Mikrotik Router OS yang terbentuk software.
- BUILT-IN hardware Mikrotik dalam bentuk perangkat keras yang khusus dikemas dalam board router yang didalamnya sudah terinstal mikrotik routerOS [12].

3. METODE PENELITIAN

Riset dilaksanakan pada bulan April s. d Juli 2023 bersamaan di Sekolah Sekolah Menengah Kejuruan(SMK) Negara 3 Payakumbuh. Penentuan tempat ini didasarkan atas estimasi kalau situasi sekolah membolehkan buat dicoba riset ini.

Tipe riset yang digunakan dalam pembuatan skripsi ini merupakan riset serta pengembangan(research and development) ataupun R & D. Dengan cara simpel tata cara riset serta pengembangan itu merupakan tata cara riset yang dipakai buat menciptakan produk khusus, dengan mencoba keberhasilan produk tersebut[2]. Buat bisa menciptakan produk khusus dipakai riset yang bertabiat analisa keinginan(dipakai tata cara survei ataupun kualitatif) serta buat mencoba keberhasilan produk itu biar bisa berperan di warga besar, hingga di perlukan riset buat menjguji keberhasilan produk tersebut(dipakai tata cara penelitian)[3]. Produk yang diperoleh berbentuk metode bentuk manajemen bandwidth memakai firewall filtering.

Produk yang dibesarkan dalam riset ini berbentuk sistem manajemen bandwidth memakai mikrotik router. Bentuk pengembangan yang dipakai merupakan PPDIIO(Prepare, Plan, Design, Implement, Operate, Optimize). Selanjutnya jenjang pada PPDIIO[4]



Gambar 1. Metode PPDIIO

Selanjutnya merupakan uraian dari tiap- tiap langkah dalam PPDIIO:

- a. Prepare

Tahap ini ialah jenjang buat memastikan keinginan badan, meningkatkan strategi jaringan serta menganjurkan rancangan srsitektur dengan tingkat tingkatan besar buat mensupport strategi sesuatu badan.
- b. Plan

Tahap ini mengenali persyaratan jaringan bersumber pada tujuan, sarana serta keinginan konsumen.
- c. Design

Konsep jaringan dibesarkan bersumber pada persyaratan teknis, serta keinginan era depan yang didapat dari situasi lebih dahulu. Jaringan itu haruslah sediakan ketersediaan, kehandalan, keamanan, skalabilitas serta kemampuan.
- d. Implement

Pada tahap ini, peralatan- peralatan terkini dicoba instalasi serta dikonfigurasi cocok detail konsep. Fitur terkini ini hendak mengubah ataupun menaikkan prasarana yang terdapat.
- e. Operate

Operasional mencakup pengurusan serta memantau bagian- bagian jaringan, mengatur aktivitas upgrade, serta mengidentifikasi serta membetulkan kekeliruan jaringan. Pada langkah ini pula dicoba pengetesan kepada jaringan yang sudah terbuat. Pengetesan dicoba dengan mengukur Quality of Service(QoS). Quality of Service(QoS) merupakan keahlian sesuatu jaringan buat sediakan layanan yang bagus dengan sediakan bandwidth, menanggulangi jitter serta delay. Patokan QoS merupakan latency, jitter, packet loss, throughput, MOS. QoS amat didetetapkan oleh mutu jaringan yang dipakai. Ada sebagian aspek yang bisa merendahkan angka

QoS, semacam: Redaman. Bias serta Noise[5]. Performansi mangacu ke tingkatan kecekatan serta keandalan penyampaian bermacam tipe bobot informasi didalam sesuatu komunikasi. Performansi ialah berkas dari beberpa patokan teknis ialah:

f. Delay

Delay merupakan durasi yang diperlukan informasi buat menempuh jarak asal ke tujuan. Delay bisa dipengaruhi oleh jarak, alat raga, penimbunan ataupun pula durasi cara yang lama. Buat mencari angka Delay, bisa memakai persamaan[5].

$$\text{Delay} = \frac{\text{total delay}}{\text{jumlah total paket}}$$

Table 1. Kategori Delay:

Kategori Degradasi	Delay(ms)	Indeks
Amat Bagus	0 ms	4
Bagus	0 s/d 75 ms	3
Sedang	75 ms s/d 125 ms	2
buruk	≥125 ms	1

g. Packet Loss

Ialah sesuatu patokan yang melukiskan sesuatu situasi yang membuktikan jumlah keseluruhan paket yang lenyap, bisa terjalin sebab collision serta congestion pada jaringan serta perihal ini mempengaruhi pada seluruh aplikasi sebab retransmisi hendak kurang efesien jaringan dengan cara totalitas walaupun jumlah bandwidth lumayan ada buat aplikasi- aplikasi itu. Biasanya fitur jaringan mempunyai buffer buat menampung informasi yang diperoleh. Bila terjalin konggesti yang lumayan lama, buffer hendak penuh serta informasi terkini tiddak hendak diperoleh. Buat mencari angka Packet Loss bisa memakai pertemuan:

$$\text{Packet Loss} = \frac{\text{paket data terkirim} - \text{paket data diterima}}{\text{paket data dikirim}} \times 100\%$$

Table 2. Kategori Packet Loss.

Kategori Degradasi	Packet Loss	Indeks
Amat Bagus	0%	4
Bagus	3%	3
Sedang	15%	2
Buruk	25%	1

h. Throughput

Throughput merupakan kecekatan(rate) tranfer informasi efisien, yang diukur dalam bps, Throughput ialah jumlah keseluruhan kehadiran paket yang dicermati pada destination sepanjang istirahat durasi khusus dipecah oleh lama istirahat durasi itu. Angka Throughput bisa dihitung memakai pertemuan.

$$\text{Throughput} = \frac{\text{jumlah data yang dikirim}}{\text{waktu pengiriman data}}$$

Table 3. Kategori Throughput.

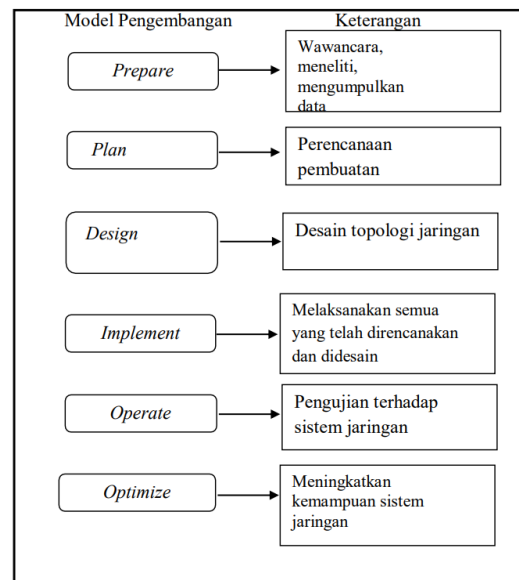
Kategori Degradasi	Throughput	Indeks
Amat Bagus	76-100%	4
Bagus	51-75%	3
Sedang	26-50%	2
Buruk	≤25%	1

i. Optimize

Tahap ini mengaitkan pemahaman proaktif seseorang manajemen jaringan dengan mengenali serta menuntaskan permasalahan saat sebelum perkara tersebut pengaruhi jaringan.

3.1. Fase Penelitian

Berikut ini merupakan skema dari tahapan penelitian:



Gambar 2. Skema Tahapan Penelitian

3.2. Uji Produk

Percobaan peoduk terbuat buat memandang keabsahan, praktilitas serta daya guna produk. Percobaan produk ini pengarang membiarkan supaya kesahian produk pengarang aman, percobaan produk terdiri dari:

Keabsahan merupakan dimensi yang membuktikan sepanjang mana instrumen juru ukur sanggup mengukur apa yang hendak diukur[6]. Keabsahan ialah bagian akurasi antara informasi yang terjalin pada subjek riset dengan informasi yang bisa dikabarkan oleh periset. Dengan begitu informasi yang asi merupakan informasi yang tidak berlainan antara informasi yang dikabarkan oleh periset dengan informasi yang sebetulnya terjalin pada subjek riset.

Buat menciptakan produk yang bermutu serta sedia dicoba hingga butuh terdapatnya percobaan keabsahan produk dalam riset ini, percobaan keabsahan dicoba oleh sebagian pakar(expert).

Pengetesan dicoba dengan menyamakan angket mengenai evaluasi dari produk.

Percobaan keabsahan dicoba dengan merujuk metode statistik Aiken' s. Metode itu semacam pada pertemuan berikut[7].

$$V = \sum \frac{s}{n(c-1)}$$

Keterangan:

- s : r-lo
- lo = nilai riset keabsahan yang terendah.
- c = nilai riset keabsahan yang paling tinggi.
- r = nilai yang diserahkan oleh seorang riset.
- n = jumlah riset.

Table 4 Kriteria Penentuan Validitas Aiken's.

Presentase %	Kriteria
0,6≤	Tidak Valid
≥=0,6	Valid

3.3. Uji Praktilitas Produk

Sehabis produk divalidasi serta hasilnya asi hingga langkah berikutnya merupakan percobaan praktikalitas. Percobaan praktikalitas ialah standar ukur dari bagian kepraktikan produk. Produk bertabat efisien bila produk itu gampang dipakai serta tidak terbelit- belit. Percobaan praktikalitas diolah memakai metode moment kappa, selaku berikut[8].

$$momentkappa(k) = \frac{p-pe}{1-pe}$$

Keterangan[13]:

- k = moment kappa yang membuktikan praktikalitas produk.
- p = nisbah yang terealisasi, di jumlah dengan metode jumlah angka yang diberi oleh pengetes dipecah jumlah angka maksimum.
- pe = propopsi yang tidak terealisasi, dihitung dengan metode jumlah angka maksimum dikurangi dengan jumlah nila keseluruhan yang diberi pengetes dipecah dengan jumlah angka maksimal.

Table 5 Kriteria Praktikalitas Moment Kappa.

Interval	Kategori
0,81 – 1,00	Amat Tinggi
0,61 – 0,80	Tinggi
0,41 – 0,60	Sedang
0,211 – 0,40	Rendah
0,00 – 0,20	Amat Rendah
≤ 0,00	Tidak Praktis

3.4. Uji Efektivitas Produk

Percobaan daya guna ialah langkah terakhir dalam pengetesan produk. Percobaan daya guna merupakan pengukuran sesuaian antara hasil produk kepada tujuan dini. Percobaan daya guna diolah dengan merujuk metode statistic Richard R. Hake(G-Score) selaku berikut[9].

$$\leq g \geq = \frac{(\% < sf > - \% < Si >)}{(100 - \% < Si >)}$$

Keterangan[13]:

- ≤g> = G-Score
- ≤Sf> = Score akhir
- ≤Si> = Score awal

Patokan tiap penanda deari lembar percobaan selaku selanjutnya[8]:

- “ High- g” daya guna besar bila memiliki(≤g>)≥0. 7.
- “ Medium- g” daya guna lagi bila memiliki 0. 7≥(≤g>)≥0. 3.
- “Low- g” daya guna kecil bila memiliki(≤g>)≤0. 3.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Penelitian

Bersumber pada hasil riset hal eksploitasi mikrotik router dengan tata cara firewall filtering yang sudah terlaksanakan, didapat hasil riset pada tiap- tiap langkah Prepare, Plan, Design, Implement, Operate serta Optimize merupakan selaku selanjutnya

4.2. prepare

Saat sebelum melaksanakan penyusunan kepada system yang terkini, butuh adanya analisa hal system yang lagi berjalan, alhasil perihal itu hendak mempermudah pengarang dalam mendefenisikan permasalahan yang mencuat dalam sistem yang lagi berjalan. Pada langkah ini pengarang melaksanakan aktivitas obsevasi di SMKN 3 Payakumbuh.

Cara yang dicoba ditahap ini merupakan menganalisa keinginan serta mengenali permasalahan pada topologi jaringan yang sudah terdapat lebih dahulu serta mengakulasi informasi ataupun data yang diperlukan dalam eksploitasi firewall filtering. Informasi diperoleh bersumber pada pada hasil pemantauan serta tanya jawab dengan pelapor yang terdapat di tempat riset.

4.3. Plan

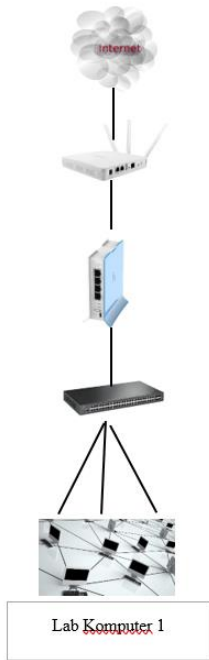
Oleh sebab itu, kegiatan dicoba pada langkah perencanaan merupakan merancang rancangan keamanan jaringan dengan tata cara firewall filtering memakai mikrotik di SMKN 3 Payakumbuh. Dengan memakai winbox dalam mengatur serta mengkonfigurasi firewall filtering memakai mikrotik.

4.4. Design

Pada langkah ini dicoba pembuatan konsep konsep jaringan tata cara firewall filtering, mulai dari pembangunan jaringan hingga pada kesiapan hardware- software yang di butuhkan semacam modem, mikrotik router, kabel UTP, laptop serta lain- lain. Ilustrasinya pada konsep topologi jaringan.



Gambari 3. Topologii Jaringani Sebelum Dii Terapkani Firwall Filtering



Gambari 4. Topologii Jaringani Sedudahi Dii Terapkani Firwall Filtering

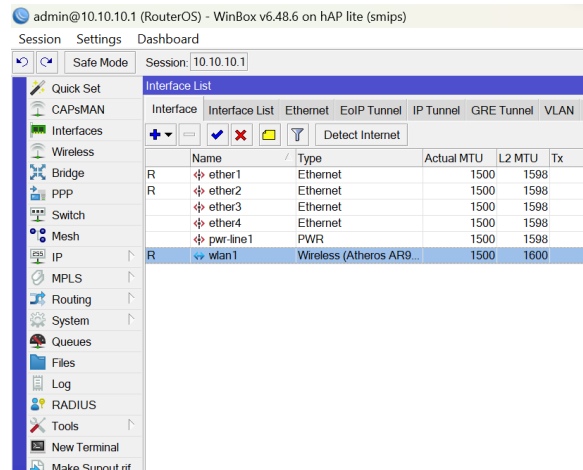
4.5. Implement pada perangkat keras

a. Instal winbox

Pada penguinstalan winbox bisa dilakukan pada link website https://mikrotik.com/download_ini.

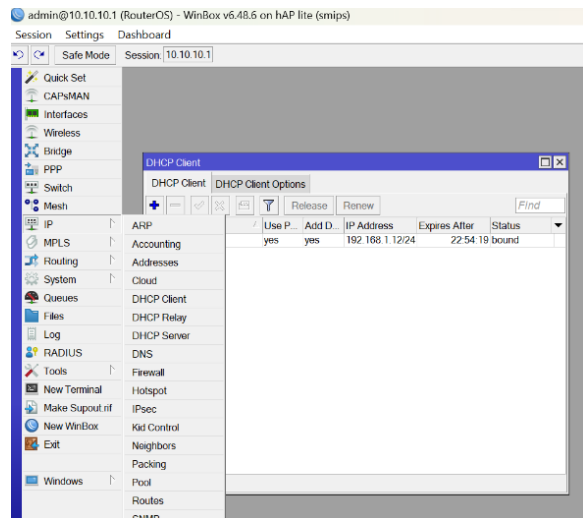
b. Konfigurasi router

Connect aplikasi winbox ke mikrotik



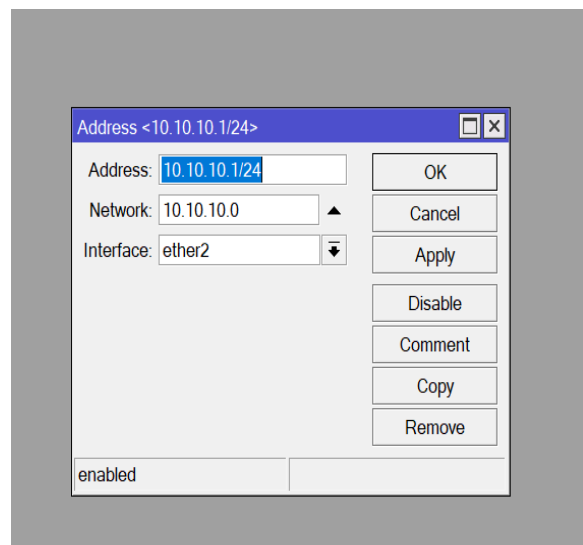
Gambar 4. Menghubungkan Internet ke Mikrotik

c. Menambahkan DHCP Client



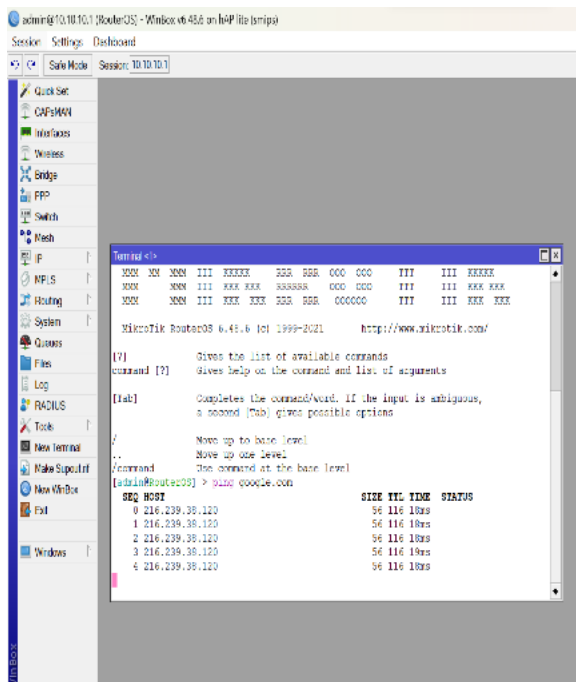
Gambar 5. Menambahkan DHCP Client

d. Membuat ip pada ether2 dengan ip 10.10.10.1/24



Gambar 6. Membuat IP Address

e. Mencoba cara ping di New Terminal

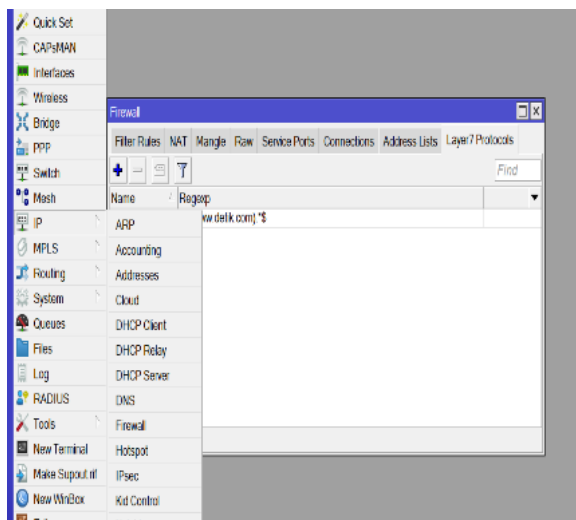


Gambar 7. Ping di New Terminal

f. Selanjutnya menghubungkan internet ke pc/laptop

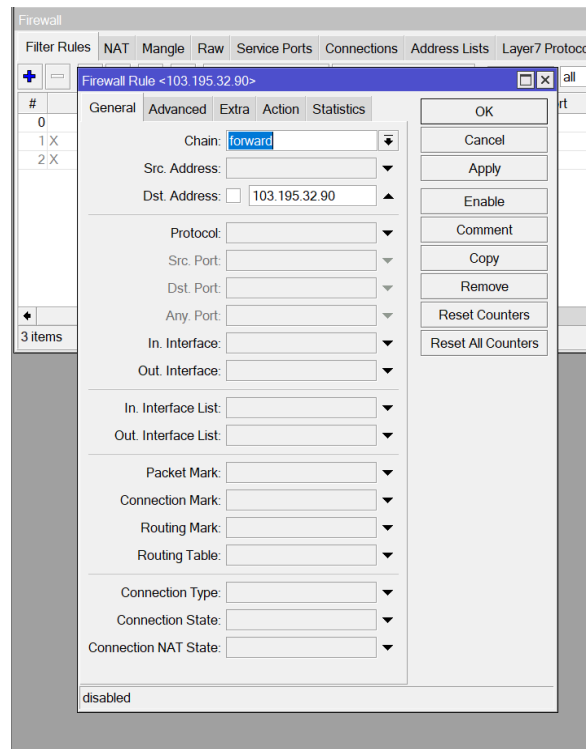
IP address : 10.10.10.2
 : 255.255.255.0
 : 10.10.10.1
 DNS server : 8.8.8.8
 : 8.8.4.4

g. Memblokir dengan Layer 7 Protocol



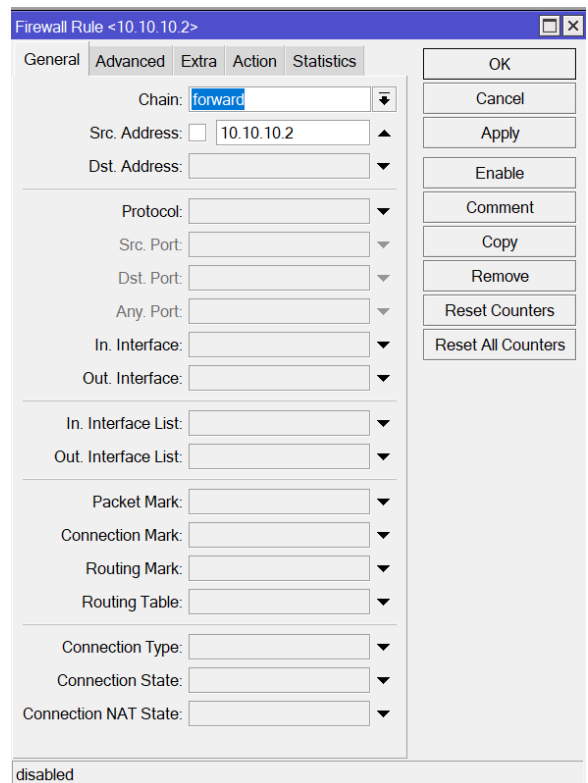
Gambar 8. Memblokir Menggunakan Layer 7 Protocol

h. Menggunakan IP Address



Gambar 9. Menggunakan IP Address

i. Memblokir ip pc/laptop agar tidak dapat mengakses internet

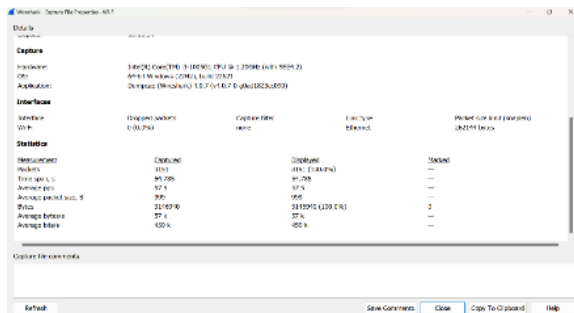


Gambar 10. Memblokir IP Pc/Laptop Agar Tidak Terhubung Ke Internet

4.6. Oprate

a. Hasil Uji *Quality of Service* (Qos)

Dalam riset ini memakai Qos mencakup delay, packet lossi serta throughput memakai aplikasi jaringan analyzer wireshark. Dalam pengetesan ini memakai laptop yang legal selaku klien, selanjutnya ini merupakan hasil informasi captur informasi oleh wireshark dengan badwidth 1 Mbps:



Gambar 11. Hasil Speedtest data oleh wireshark

Dari captur yang sudah dicoba dengan wireshark dengan bandwidth 1 Mbps diperoleh angka kalkulasi selaku selanjutnya:

b. *Delay*

$$\begin{aligned} \text{Rata-rata Delay} &= \text{Total Delay} / \text{Jumlah Total Paket} \\ &= 54785271 \text{ sec} / 3150 \\ &= 17392149.5238 \text{ sec} \\ &= 17.392 \text{ ms} \end{aligned}$$

c. *Packet Loss*

$$\begin{aligned} \text{Packet Loss} &= \text{Paket data dikirim} - \text{paket data diterima} / \text{paket data dikirim} \times 100\% \\ &= 3151 - 3151 / 3151 \times 100\% \\ &= 0\% \end{aligned}$$

d. *Throughput*

$$\begin{aligned} \text{Throughput} &= \text{Jumlah data yang dikirim} / \text{waktu pengiriman data} \\ &= 3146940 \text{ bytes} / 54785 \text{ sec} \\ &= 57.4416354842 \text{ bytes/sec} \\ &= 45953.30838736 \text{ Kbps} \end{aligned}$$

$$\begin{aligned} \% \text{Throughput} &= \text{Throughput} / \text{Alokasi Bandwidth User} \times 100\% \\ &= 45953.30838736 \text{ Kbps} / 1024 \text{ Kbps} \times 100\% \\ &= 44\% \end{aligned}$$

Sehabis dicoba kalkulasi diperoleh angka akhir Qos bisa diamati pada table selanjutnya:

Table 6. Nilai Akhir Qos (Quality of Service)

Parameter Qos	Indeks	Kstegori
<i>Delay</i>	3	Bagus
<i>Packet Loss</i>	4	Amat Bagus
<i>Throughput</i>	2	Sedang
Total Rata-rata	3	Bagus

Bersumber pada table diatas angka dari Qos indikator merupakan 3 dengan jenis baik. Dari hasil informasi yang diperoleh pada aplikasi Wireshark, serta setelah itu di suguhkan dalam wujud table pada lukisan diatas, bisa diamati angka keseluruhan pada umumnya patokan delay sebesar 17.392ms dengan jenis“ Baik” angka delay amat mempengaruhi kepada seberapa besar bandwidth yang diserahkan, hingga hendak terus menjadi kecil angka delay yang diperoleh.

Hasil dari Packet Loss mempunyai patokan 0% dengan jenis“ Amat Baik”. Packet Loss dipakai buat mengenali banyak julah paket yang lenyap ataupun tidak hingga ke tujuan kala melaksanakan pengiriman informasi dari pangkal ke tujuan.

Hasil dari angka Throughput dimana patokan sebesar 44% dengan jenis“ Lumayan”. Dari table diatas, Throughput dipakai buat mengenali jumlah paket yang diperoleh dalam kondisi bagus kepada durasi keseluruhan transmisi yang diperlukan dari server sampai ke user. Hasil analisa Packet Loss mempunyai patokan sebesar 0%.

4.7. Percobaan Keabsahan Produk

Buat mendapatkan hasil yang bermutu serta sedia digunakan, butuh dicoba percobaan keabsahan produk. Percobaan keabsahan dicoba buat memandang isi dari produk itu dengan tujuan buat memandang akurasi isi produk. Langkah pengetesan keabsahan ini pengarang tujuan pada pakar dalam aspek pc ialah Ayah Firdaus Annas, S. Pd, Meter. Kom, Ayah Riri Okra, Meter. Kom serta ibuk Yulifda Elin Yuspita, Meter. Kom.

Sehabis melaksanakan kalkulasi kepada hasil dari lembar pengesahan, hingga keamanan jaringan dengan metodde firewall filtering memakai mikrotik di SMKN 3 Payakumbuh ini memperoleh angka 0, 84 angka itu buat memastikan keabsahan angkat“ V” didapat antara 0. 00 hingga 1. 00. jenis determinasi keabsahan resep Aiken’ s V besar serupa dari 0. 60 serta tidak valid bila angka Aiken’ s V kecil dari 0. 60, hingga angka dari sistem ini merupakan valid.

4.8. Percobaan Praktikalitas Produk

Percobaan praktikalitas keamanan jaringan dengan tata cara firewall filtering memakai mikrotik router RB941 di SMKN 3 Payakumbuh ini didapat bersumber pada lembar praktikalitas yang diisi oleh 5 orang guru pc sang SMKN 3 Payakumbuh. Dari 5 guru itu di dapat angka 0, 91 dengan begitu keamanan jaringan dengan tata cara firewall filtering memakai mikrotik di SMKN 3 Payakumbuh yang sudah pengarang untuk merupakan amat efisien.

4.9. Percobaan Daya guna Produk

Percobaan daya guna keamanan jaringan dengan tata cara firewall filtering memakai mikrotik router RB941 di SMKN 3 Payakumbuh ini bersumber pada lembar daya guna yang diisi oleh pengetes, ialah pada 8 anak didik SMKN 3 Payakumbuh. Riset dengan cara biasa kepada produktif ini amat efisien dengan angka

0, 84 cocok dengan adendum angket daya guna produk.

4.10. Optimize

Pada langkah ini dicoba sesuatu wujud upaya yang dicoba buat mengalami kasus yang hendak dialami keamanan jaringan dengan tata cara firewall filtering memakai mikrotik di SMKN 3 Payakumbuh sehabis berakhir dicoba, semacam sebagian perihal di dasar ini:

- Mengaitkan jaringan internet ke komputer atau laptop lewat mikrotik router RB941.
- Memblokir suatu web, perihal ini dicoba buat menjauhi para konsumen menyalahgunakan jaringan internet.
- Memblokir suatu ip komputer atau laptop, perihal ini dicoba supaya komputer atau laptop betul-betul terpenggal ke jaringan internet.

4.11. Pembahasan

Hasil riset ini merupakan keamanan jaringan dengan tata cara firewall filtering memakai mikrotik router RB941 di SMKN 3 Payakumbuh. Berlainan dengan riset lebih dahulu, pada riset ini pengarang berpusat pada keamanan jaringan dengan tata cara firewall filtering dimana supaya user tidak bisa membuka suatu web ataupun akses internet yang terkoneksi ke jaringan.

Selaku hasil riset dicoba percobaan pengesahan dari produk ini didapat bersumber pada lembar pengesahan yang diisi oleh validator. Dari hasil evaluasi validator memperoleh hasil yang asi dengan angka 0, 84. Setelah itu pada percobaan praktikalitas memperoleh hasil efisien dengan angka 0, 91. Serta pada percobaan daya guna diperoleh hasil efisien dengan angka 0, 84. Jadi, tujuan pembuatan skripsi ini merupakan buat menolong pihak sekolah dalam keamanan jaringan dengan tata cara firewall filtering memakai mikrotik di SMKN 3 Payakumbuh.

Sehabis dikerjakannya penghentian suatu web ataupun web lain memakai firewall filtering memakai mikrotik bisa diperoleh kalau web itu dapat di membekukan. Perihal itu cocok dengan yang di sampaikan oleh Arandha Aryanto Astari (2018) dalam riset hal“ Aplikasi Keamanan Jaringan Dengan Tata cara Firewall Filtering Memakai Mikrotik”. Yang dimana mangulas mengenai pengaturan firewall serta rule yang di pastikan.

Riset ini mempraktikkan tipe riset memakai PPDIOO(Prepare, Plan, Design, Implement, Operate, Optimize) hal eksploitasi mikrotik router dengan tata cara firewall filtering. Perihal itu berlainan dengan Efrahim Sinyo Rio Ola Balen Langobelen(2019) dalam riset hal“ Analisa Serta Optimasi Dari Imitasi Keamanan Jaringan Memakai Mikrotik Riset Permasalahan Di Halaman Cerdas Yogyakarta”. Diperoleh bahwa bentuk buat firewall, pengurusan service port serta bentuk penapis buat Bridge. Perihal itu dipaparkan dengan cara nyata dalam hasil serta

ulasan riset ini yang dilengkapi dengan ujicoba permasalahan dari tiap- tiap ulasan.

Riset yang dicoba pengarang cuma memakai firewall filtering memakai router mikrotik sebaliknya pada riset yang dicoba oleh Iguti Komang, Oka Madiyana(2015) hal“ Keamanan Jaringan Dengan Firewall Penapis Berplatform Mikrotik Pada Makmal Pc Stikom Bali”. Diperoleh kalau dalam melaksanakan packet penapis cocok dengan keinginan pada keinginan Makmal Pc STIKOM Bali sanggup mengamankan jaringan pada Makmal Pc dengan melaksanakan penapis kepada lau rute informasi yang melampaui router cocok dengan determinasi yang sudah didesain.

Dalam riset ini hasil percobaan Quality of Service(Qos) mencakup delay, packet loss serta throughput memakai aplikasi jaringan analyzer wireshark. Perihal itu berlainan dalam riset yang dicoba oleh Sumardi Jayanto, Ahmad Tantoni serta Hasyim Asyari(2021) yang hal“ Implentasi Keamanan Jaringan Dengan Packet Filtering Berplatform Mikrotik Buat Internet Positif Di SMKN 1Praya”. Melaksanakan pengetesan saat sebelum membuat suatu sistem yang sanggup memblokir sebagian aplikasi yang melampaui jaringan.

Dalam riset ini pengarang melaksanakan penghentian dengan memakai Layer 7 Protocol, ip address serta ip komputer atau laptop buat menyudahi ataupun memblokir sesuatu web dari jaringan. Perihal itu berlainan dengan yang di informasikan oleh Mhd. Ajaran, Alat Gunawan serta Zulia Almadi Siregar(2022) dalam riset hal“ Keamanan Jaringan Wlan Dengan Tata cara Firewall Filtering Memakai Mikrotik Pada SMP Negara 1 Dolok Merawan”. Yang dimana pembahasannya memakai Layer 7 Protocol serta website proxy yang ialah salah satu tata cara dalam penghentian.

5. KESIMPULAN DAN SARAN

Bersumber pada hasil riset yang pengarang jalani serta uraikan yang sudah pengarang jalani pada bab-bab lebih dahulu, hal keamanan jaringan dengan tata cara firewall filtering memakai mikrotik di SMKN 3 Payakumbuh, hingga disimpulkan kalau keamanan jaringan dengan tata cara firewall filtering bisa mengoptimalkan dalam cara berlatih membimbing di SMKN 3 Payakumbuh supaya user tidak bisa melaksanakan penyalahgunaan jaringan kala dalam cara berlatih membimbing. Tidak cuma itu penghentian suatu web web, sosial alat ataupun permainan oline serupanya dengan tata cara firewall filtering memakai mikrotik router RB941 tidak bisa di search dimanapun supaya dapat mengoptimalkan dalam cara berlatih membimbing. Eksploitasi mikrotik router sudah bisa menuntaskan permasalahan yang sudah pengarang rumuskan pada bagian kesimpulan permasalahan, lewat pengetes produk dengan memakai angket pada pakar aspek pc, guru serta anak didik alhasil diperoleh hasil produk yang asi, efisien serta efisien.

DAFTAR PUSTAKA

- [1] N. Y. Saprianto, "Manajemen Bandwidth dengan Mikrotik Pada Dinas Pendidikan Surabaya," *J. Univ. Din.*, p. 83, 2020, [Online]. Available: <https://repository.dinamika.ac.id/id/eprint/5065/1/14410200060-2020-UNIVERSITASDINAMIKA.pdf>
- [2] B. Fasehan, "Rancang Bangun Sistem Keamanan Jaringan Komputer Menggunakan Firewall Filter Pada Laboratorium Jurusan Teknik Komputer," p. 13, 2020.
- [3] I. Dwinanto and H. Setiyani, "Implementasi Keamanan Komputer pada Aspek Confidentiality, Integrity, Availability (CIA) Menggunakan Tools Lynis Audit System," *J. Maklumatika*, vol. 8, no. 1, pp. 35–46, 2021.
- [4] S. W. Deni Lestiono, "Konsep Penerapan Keamanan Jaringan Publik Di Lingkungan Kampus Stmik Bina Patria," *Transformasi*, vol. 16, no. 1, pp. 91–101, 2020, doi: 10.56357/jt.v16i1.220.
- [5] E. Ramadhani, "Eksplorasi Isu Keamanan Jaringan Wireless Studi Kasus Universitas Gadjah Mada," *Media Inform.*, vol. 7, no. 2, p. 12, 2014, [Online]. Available: https://www.researchgate.net/profile/Erika-Ramadhani/publication/303382812_EKSPLOKASI_ISU_KEAMANAN_JARINGAN_WIRELESS_STUDI_KASUS_UNIVERSITAS_GADJAH_MADA/links/573f7aa508ae298602e8f517/EKSPLOKASI-ISU-KEAMANAN-JARINGAN-WIRELESS-STUDI-KASUS-UNIVERSITAS-GADJA
- [6] D. B. Rendo, Ngatono, and W. N. Aji, "Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus Di Smk Negeri 1 Kota Serang)," *PROSISKO*, vol. 7, no. 2, pp. 108–115, 2020.
- [7] M. Ilham, I. Gunawan, and Z. A. Siregar, "Keamanan Jaringan Wlan Dengan Metode Firewall Filtering Menggunakan Mikrotik Pada Smp Negeri 1 Dolok Merawan," *J. Ilm. Sist. Inf. Dan Ilmu Komput.*, vol. 2, no. 3, p. 16, 2022, doi: <https://doi.org/10.55606/juisik.v2i3.309>.
- [8] M. F. W. A. Wahyu, "Penerapan Firewall Menggunakan Fortigate di PT.PLN Rayon Taman Sidoarjo," *Universitas Dinamika*. p. 7, 2019. [Online]. Available: <https://repository.dinamika.ac.id/id/eprint/3878/>
- [9] D. A. Jakaria and A. Yulianeu, "Implementasi Firewall Dan Web Filtering Pada Mikrotik Routeros Untuk Mendukung Internet Sehat Dan Aman (Insan)," *J. Jutekin*, vol. 8, no. 2, p. 8, 2020, doi: <http://dx.doi.org/10.51530/jutekin.v8i2.480>.
- [10] Didi Susianto, "Implementasi Queue Tree Untuk Manajemen Bandwidth Menggunakan Router Board Mikrotik," *J. Cendikia Vol 12No. 1Cendikia 2016 ISSN 0216-9436 Bandar Lampung, April 2016*, vol. 12, no. 1, pp. 1–8, 2019.
- [11] Romulo Parlindungan Aritonang, R. Nasution, and I. Giawa, "Konfigurasi Voucher Internet dengan Mikrotik Server dan Mikrotik Routerboard Pada Jaringan Komputer Institut Teknologi dan Bisnis Indonesia," *J. Inform. Dan Peranc. Sist.*, vol. 5, no. 1, p. 8, 2023, [Online]. Available: <https://jurnal.itbi.ac.id/index.php/journalinformatika/article/view/92/48>
- [12] A. Munawar, "Penggunaan Mikrotik Router Os Untuk Mengkonfigurasi Gateway Server Dan Management Bandwidth Dalam Membangun Jaringan Komputer Di Kos Bpk. Suwarjo," p. 20, 2012, [Online]. Available: https://repository.amikom.ac.id/files/Naskah_Publikasi_07.11.1792.pdf
- [13] M. R. Darmawan and H. A. Musril, "Perancangan Sistem Pendaftaran Audiens Seminar Proposal di Institut Agama Islam Negeri (IAIN) Bukittinggi," *J. Teknol. dan Inf.*, vol. 11, no. 1, pp. 26–39, 2021, doi: 10.34010/jati.v11i1.3346.