BAB II TINJAUAN PUSTAKA

2.1. PENELITIAN SEBELUMNYA

Penelitian mengenai implementasi dan pengembangan jaringan *internet* berbasis *router mikrotik* bukan pertama kali dilakukan. Dalam bab ini, penulis menjabarkan penelitian-penelitian terkait dengan penelitian ini yang akan menjadi referensi.

Salah satu penelitian terkait tahun 2022, yaitu berjudul "Pembangunan Jaringan Hotspot Berbasis *Mikrotik* pada Kampung Tematik di Kecamatan Padang Utara" yang ditulis oleh Hadi Syahputra dan Romi Wijaya [11]. Pada penelitian tersebut pembangunan jaringan *hotspot* berbasis *mikrotik* kemudian dalam pembangunan jaringan tersebut menggunakan metode pelaksanaan adalah dengan membangun jaringan *hotspot* berupa tower yang berbasis *mikrotik* sebagai lalu lintas jaringan, pemberian IP (DHCP) yang dibantu dengan perangkat jaringan lainnya, seperti *modem*, *acces point*, kabel utp, *Wireless*, laptop, dll. Hasil yang didapatkan pada penelitian tersebut yaitu telah berhasil diterapkan di Kampung Tematik Kecamatan Padang Utara sebagai solusi dari masalah mahalnya biaya untuk membeli kouta *internet* [11].

Penelitian lainnya pada tahun 2022, yaitu berjudul "Pemanfaatan Mikrotik Routerboard Untuk Optimasi *Bandwidth* dan Keamanan Jaringan Di PT. Semen Baturaja (Persero) TBK" yang ditulis oleh Tamsir Ariyadi dan Moh Rizki Alfyuddin [12]. Dalam penelitian ini, metode yang diterapkan adalah melakukan diagnosis, yang memiliki tujuan dengan permasalahan yang hendak dipecahkan dan merancang rencana tindakan dengan tujuan memahami inti dari permasalahan yang ada kemudian melanjutkan dengan menyusun rencana tindakan yang sesuai. Berdasarkan hasil penelitian ini setelah diterapkan *Manajemen Bandwidth*, yang bertujuan memberikan *bandwidth* yang ideal pada jaringan *internet* PT. Semen Baturaja (Persero) Tbk Palembang karena dapat membagi *bandwidth* secara adil pada setiap ruang, kemudian *Radius Server*, yang bertujuan membuat keamanan jaringan

sebagai autentikasi koneksi sebelum menggunakan ISP yang tersedia dan *Access Filter*, yang bertujuan tidak dapat menambah jumlah besar *bandwidth* tetapi memfilter konten yang akan dibuka oleh *user*/karyawan [12].

Penelitian lainnya pada tahun 2021, yaitu berjudul "Perancangan Sistem Keamanan Jaringan Menggunakan Mikrotik *Router* Pada *Management Bandwidth* di CV. Algi Pin Bandung" yang ditulis oleh Deri Andriyana Juhana, Soecipto, dan Ani Amaliyah [14]. Penelitian ini menerapkan pendekatan deskriptif. Metode yang digunakan adalah *Network Development Life Cycle (NDLC).* Pada penelitian ini memiliki masalah di CV. Algi Pin menghadapi tantangan terkait dengan struktur jaringan yang tidak teratur dan koneksi internet yang lambat. Selain itu, belum ada pembagian *bandwidth* yang tepat untuk setiap *access point*, dan alokasi *bandwidth* untuk pengguna yang berbeda masih belum terorganisir dengan baik, mengakibatkan hak akses yang tidak optimal. Permasalahan lainnya terkait dengan akses ke perangkat wifi dalam jaringan, di mana sistem *login* hanya mengandalkan keamanan berbasis Wired Equivalent Privacy (WEP), yang dianggap belum memadai dalam hal keamanan. Penelitian ini bertujuan untuk menciptakan desain sistem keamanan jaringan dengan memanfaatkan router Mikrotik pada manajemen bandwidth, serta meningkatkan optimalisasi keamanan sistem *login* jaringan di CV. Algi Pin, sehingga pengguna dapat merasa lebih aman dalam menggunakan layanan tersebut. Dampaknya adalah jaringan komputer CV Algi Pin dapat mencapai tingkat optimalitas yang lebih baik karena setiap unit memiliki alokasi bandwidth masing-masing. Keamanan jaringan CV Algi Pin juga telah diperbarui, menghilangkan kekhawatiran terhadap serangan luar, dan administrator memiliki kemampuan untuk mengontrol serta mengurangi beban bandwidth, memblokir akses ke media sosial, dan game. [14].

Penelitian lainnya pada tahun 2021, yaitu berjudul "Implementasi Jaringan *Hotspot* Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer" yang ditulis oleh Mokhamad Gustiawan, Ristu Juli Yudianto, Johanes Pratama, dan Abdurahman Fauzi [15]. Tujuan dari penelitian ini

adalah menerapkan jaringan hotspot di lingkungan perkantoran agar kantor dapat menyediakan layanan hotspot menggunakan Mikrotik. Selain itu, penelitian ini bertujuan untuk mendistribusikan bandwidth secara adil di jaringan hotspot kepada setiap pengguna dan membatasi penggunaan bandwidth sesuai dengan waktu yang tercantum pada voucher paket. Dari hasil penelitian ini, implementasi jaringan hotspot menggunakan Mikrotik RouterOS telah dilakukan yang berfungsi dapat meningkatkan efisiensi kinerja jaringan dengan optimalisasi penggunaan bandwidth pada hotspot. Dengan menggunakan Mikrotik RouterOS dalam jaringan hotspot, administrator memiliki kemampuan untuk mengontrol dan membatasi penggunaan bandwidth secara merata [15].

Penelitian lainnya pada tahun 2021, yaitu berjudul "Penerapan Sistem Autentikasi dan Pengamanan pada Jaringan *Hotspot* Berbasis *Captive Portal* di Universitas Prof. Dr. Hazairin, SH" yang ditulis oleh Elviza Diana, Ade Fitrah Putra Akhir, dan Yulia Darmi [6]. Penelitian ini memiliki permasalahan yaitu orang umum yang mudah terhubung ke sistem *hotspot* di Universitas Prof. Dr. Hazairin, SH (UNIHAZ) dan memiliki kekurangan keamanan pada sistem jaringan *hotspot*. Metode yang digunakan yaitu *Network Develpoment Life Cycle (NDLC)* dengan tahapan analysis, desain, simulation, prototyping, implementation, monitoring dan yang terakhir manajemen. Hasil dari riset ini yaitu dengan adanya *Captive Portal* dapat meringankan tugas administrator dalam memonitor dan mengelola pengguna yang terkoneksi ke jaringan serta administrator dapat melakukan pembatasan *bandwidth*, penggunaan *Captive Portal* juga dianggap sebagai opsi yang cukup aman untuk melindungi data pengguna. Hal ini disebabkan oleh pemanfaatan *Captive Portal* dalam sistem *tunelling* menggunakan SSL, yang dapat mengenkripsi semua data yang hendak dikirimkan [6].

Penelitian lainnya pada tahun 2021, yaitu berjudul "Prototipe Manajemen Keamanan Jaringan di Pesantren (Study Kasus Pesantren Madinatunnajah)" yang ditulis oleh Abdul Majid [16]. Penelitian ini bertujuan membangun metode jaringan yang bisa memberikan perlindungan verifikasi

untuk pengguna serta manajemen *bandwidth*. Hasil riset ini menggunakan metode *Network Development Life Cycle (NDLC).* Riset ini adalah menciptakan metode perlindungan jaringan yang mempunyai kemampuan berjalan optimal dengan tingkat keberhasilan sekitar 82,5% dan memenuhi kebutuhan jaringan di Pondok Pesantren Madinatunnajah. Dengan adanya metode verifikasi perlindungan bagi *user* yang terkoneksi jaringan maka sistem jaringan bisa dimonitoring dan bisa mengelola layanan apapun yang dapat dijangkau oleh pengguna sehingga sistem jaringan di Pondok Pesantren Madinatunnajah dapat dimanajemen lebih baik dari pada sistem sebelumnya [16].

Penelitian lainnya pada tahun 2023, yaitu berjudul "Meningkatkan Keandalan Komunikasi Perlindungan dalam *Slice* 5G" yang ditulis oleh Petra Raussi , Heli Kokkoniemi-Tarkkanen , Kimmo Ahola , Antti Heikkinen , dan Mikko Uitto [17]. Penelitian ini bertujuan menganalisis pembuatan lalu lintas dan uplink menurut jawaban komersial yang ada digunakan untuk metodologi memprioritaskan komunikasi perlindungan dalam 5G. Penelitian ini menggunakan metode *quality of service* (Qos). Riset ini menghasilkan bahwa mempertahankan QoS untuk aplikasi pembentukan lalu lintas sangat penting untuk diimplementasikan di router nirkabel atau di perangkat jaringan utilitas, terutama dalam kasus dimana satu koneksi nirkabel digunakan untuk berbagai aliran informasi.

Dari uraian diatas, dapat diamati bahwa rangkuman penelitian yang relevan tercantum pada tabel dibawah ini :

Tabel 2.1. Penelitian Terdahulu

No	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
1	Perancangan Sistem Keamanan Jaringan Menggunakan Mikrotik Router Pada Management Bandwidth di CV. Algi Pin Bandung	2021 [14]	Network Development Life Cycle (NDLC)	terstruktur dan koneksi *internet* yang lambat, serta belum adanya pembagian *bandwidth* tiap *access point*.	karena telah memiliki pembagian *bandwidth* secara merata, memiliki keamanan lebih baik dari sebelumnya berupa panel *login*, dan dapat memblokir *social media* dan game.	*Cycle (NDLC)* sedangkan penelitian yang akan dilakukan menggunakan metode *hierarchical token bucket* sehingga *bandwidth* yang tersisa bisa di alihkan untuk *user* yang lebih diprioritaskan.
2	Implementasi Jaringan Hotspot Di Perkantoran	2021 [15]	Simple Queue	Masih terjadi tarik menarik *bandwidth* antar pelanggan	Metode simple queue telah berhasil membagi *bandwidth*	Penelitian sebelumnya menggunakan metode *simple queue*, sedangkan penelitian yang akan dilakukan

No	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
	Guna Meningkatkan Keamanan Jaringan Komputer.			karena pembagian *bandwidth* yang Belum merata	secara merata ke setiap *user* sehingga tidak terjadi tarik menarik *bandwidth* antar user.	menggunakan metode *hierarchical token bucket* sehingga *bandwidth* yang tersisa bisa di alihkan untuk user yang lebih diprioritaskan.
3	Penerapan Sistem Autentikasi dan Pengamanan pada Jaringan Hotspot Berbasis Captive Portal di Universitas Prof. Dr. Hazairin, SH	2021 [6]	Network Development Life Cycle (NDLC)	Orang umum mudah terhubung ke jaringan *internet*, Keamanan jaringan *internet* di Universitas Prof. Dr. Hazairin, SH Bengkulu masih belum maksimal.	Dengan mengimplementasikan captive portal yang dikembangkan membuat admin dapat mengontrol pengguna yang terhubung ke jaringan internetnya serta dapat membatasi *bandwidth*.	Penelitian sebelumnya menggunakan metode *Network Development Life Cycle* (NDLC) sedangkan penelitian yang akan dilakukan menggunakan metode *hierarchical token bucket* sehingga *bandwidth* yang tersisa bisa di alihkan untuk *user* yang lebih diprioritaskan.

No	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
4	Prototipe Manajemen Keamanan Jaringan di Pesantren (Study Kasus Pesantren Madinatunnajah)	2021 [16]	*Network Development Life Cycle* (NDLC)	Masalah dalam penelitian ini adalah otentikasi *user*, manajemen *user hotspot*, pengaturan *bandwidth* dan adanya orang mudah	Dengan adanya keamanan *captive portal*, membuat admin lebih mudah mengotentikasi pengguna dan monitoring serta manajemen terhadap pengguna yang terhubung ke jaringan	Penelitian sebelumnya menggunakan metode *Network Development Life Cycle (NDLC)* sedangkan penelitian yang akan dilakukan menggunakan metode *hierarchical token bucket* sehingga *bandwidth* yang tersisa bisa di alihkan untuk *user* yang lebih diprioritaskan.
5	Pembangunan Jaringan Hotspot	2022 [11]	Persiapan, *screening*,	Mahalnya biaya untuk membeli	Hasil sistem jaringan berbasis *mikrotik* telah	Penelitian sebelumnya tidak menggunakan *captive portal*, sedangkan penelitian yang

No	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
	Berbasis Mikrotik Pada Kampung Tematik di Kecamatan Padang Utara		implementasi kegiatan, diskusi dan ceramah, demonstrasi dan praktek, dokumentasi, dan evaluasi.	kouta internet.	berhasil diterapkan di Kampung Tematik Kecamatan Padang Utara.	akan dilakukan menggunakan *captive portal* sehingga *user* yang tidak sah tidak bisa mengakses jaringan internet tanpa adanya *username* dan *password* yang diberikan dari administrator.
6	Pemanfaatan *Mikrotik Routerboard* Untuk Optimasi *Bandwidth* dan Keamanan Jaringan Di PT.	2022 [12]	*Simple queue*	Kecepatan *internet* yang belum maksimal karena sering terjadi beban trafik yang berlebih.	Penerapan Manajemen *bandwidth* memberikan *bandwidth* yang optimal karena membagi secara seimbang.	Penelitian sebelumnya menggunakan metode *simple queue,* sedangkan penelitian yang akan dilakukan menggunakan metode *hierarchical token bucket*

No	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
	Semen Baturaja (Persero) Tbk				keamanan pada jaringan sebagai autentikasi, *Acces Filer* memfilter konten yang akan dibuka oleh *user*.	sehingga *bandwidth* yang tersisa bisa di alihkan untuk
7	Improving Reliability of Protection Communication in a 5G Slice	2023 [17]	QoS (*Quality of Service*)	Masalah penelitian ini adalah tren terbaru bahwa 5G dapat mencakup semua aplikasi smart grid yang tidak memiliki perincian yang diperlukan.	Bahwa untuk mempertahankan QoS yang baik untuk aplikasi kritis, pembentukan lalu lintas sangat penting untuk diimplementasikan di router nirkabel	Penelitian sebelumnya menggunakan metode QoS sedangkan penelitian yang akan dilakukan menggunakan metode *hierarchical token bucket* sehingga *bandwidth* yang tersisa bisa di alihkan untuk *user* yang lebih diprioritaskan.

2.2. LANDASAN TEORI

Dalam penelitian ini, beberapa teori yang diperlukan untuk mendukung kegiatan yang dilakukan. Landasan teori yang diajukan mencakup konsep dasar dan definisi terkait dengan perangkat yang digunakan sebagai elemen pendukung dalam melaksanakan penelitian ini.

2.2.1. Jaringan *Internet*

Interconnected Networking atau *Internet* merupakan jaringan-jaringan global yang tersebar diseluruh dunia dan perangkat yang saling terkoneksi menggunakan protokol komunikasi untuk bertukar informasi dan data. *Internet* membuat orang bisa untuk berkomunikasi menggunakan berbagai sosial media, melakukan transaksi bisnis dan mengakses sumber daya online seperti situs web, aplikasi dan layanan. *Internet* dapat diakses melalui berbagai perangkat seperi komputer, smartphone, tablet dan perangkat lainnya yang memiliki koneksi *internet* seperti *Wi-Fi*, kabel, atau melalui jaringan seluler [18].

2.2.2. Keamanan Jaringan

Keamanan jaringan adalah langkah-langkah yang diambil untuk melindungi jaringan komputer atau jaringan *internet* dari ancaman dan serangan yang berpotensi merusak atau merugikan pihak tertentu. Keamanan jaringan merupakan aspek yang penting dalam pengelolaan jaringan *internet* dan harus diterapkan secara komprehensif untuk melindungi data penting, sistem, dan sumber daya yang ada dalam jaringan *internet* dari ancaman yang ada [19]. Tiga (3) diantaranya yang akan menjadi konsen penelitian ini adalah tentang penggunaan *captive portal*, implementasi *web filtering* menggunakan *firewall filter* dan manajemen *use*r pada *mikrotik* menggunakan *username*.

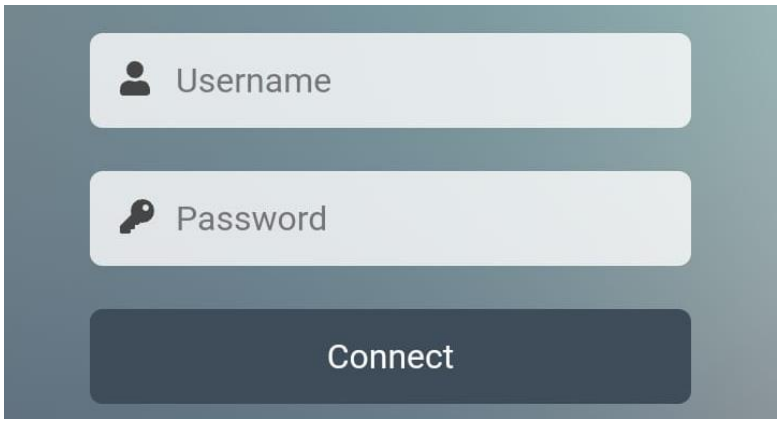
2.2.3. Web Filtering

Web filtering merupakan proses untuk membatasi atau mengatur akses pengguna jaringan *internet* terhadap web serta konten yang tersedia di *internet*. Ini dilakukan dengan menerapkan aturan yang memungkinkan hanya konten tertentu yang diizinkan atau diblokir. Tujuan dari web filtering ini adalah melindungi pengguna jaringan *internet* dari *website* yang berbahaya serta pembatasan akses untuk *website* tertentu terutama sumber *virus* jaringan. Mikrotik menyediakan fitur tersebut yaitu *firewall layer 7 proto*col seperti mengontrol situs web berdasarkan konten, *URL filtering* seperti memblokir situs web berdasarkan *URL* atau istilah kata kunci tertentu, *web proxy* seperti memblokir media sosial atau berita tertentu, *DNS filtering* seperti mencegah akses ke situs web yang tidak di inginkan, *content filtering* seperti memfilter konten dewasa atau tidak pantas, dan *layer7 protocol* seperti memfilter HTTP, HTTPS, FTP, DNS dan sebagainya [20].

2.2.4. Penggunaan Username dan Password

Saat ini, setiap perusahaan atau instansi menggunakan jaringan *internet* sebagai penunjang pekerjaan mereka. Untuk membuat akses *internet* yang tersedia menjadi kenyamanan, harus mengikuti serangkaian panduan keamanan yang ditujukan untuk meminimalisir penggunaan jaringan *internet* oleh orang yang tidak bertanggung jawab untuk aktivitas terlarang. Secara cepat, dapat membuat autentikasi portal untuk pengguna yang ingin mengakses jaringan *internet*. Dengan autentikasi portal, perangkat yang akan terhubung ke jaringan *internet* akan dimintai username dan password pengguna. Username dan password hanya dapat diberikan oleh admin yang telah memberikan izin akses *internet*, sehingga admin dapat

mengetahui pengguna siapa saja yang mengakses ke jaringan *internet*nya. Dengan demikian penggunaan username dan password saat akan mengakses *internet* dapat memberikan keamanan dan kenyamanan saat menggunakan jaringan *internet* [21].



Gambar 2.1. Penggunaan Username dan Password.

2.2.5. Bandwidth

Bandwidth adalah ukuran kecepatan koneksi *internet*. Bandwidth menunjukan seberapa data yang dapat dikirim atau diunduh dari *internet* dalam periode waktu tertentu. Semakin besar *bandwidth*, semakin banyak data yang dapat dikumpulkan atau diakses di transfer dalam satu waktu, dan semakin cepat data tersebut dapat dikirim dan diterima, apabila semakin kecil *bandwidth* maka semakin lambat transfer data tersebut [22].

2.2.6. Manajemen Bandwidth

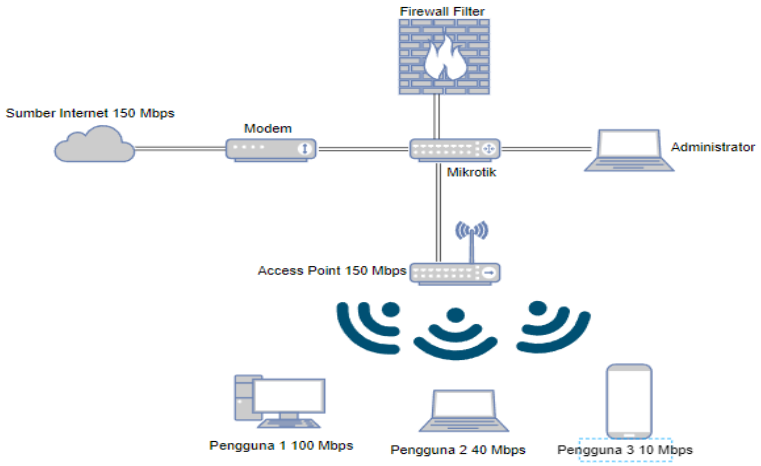
Manajemen *bandwidth* adalah proses dan menentukan besaran *bandwidth* untuk setiap pengguna pada jaringan komputer sehingga dapat memprioritaskan lalu lintas yang lebih penting atau memberikan batasan pada lalu lintas yang kurang penting dan dapat membantu dalam menjaga stabilitas kinerja jaringan [23].

2.2.7. Manajemen User

Manajemen *user* adalah proses mengelola, mengatur dan membuat akun untuk pengguna dalam suatu sistem. Manajemen user memiliki database yang dapat digunakan untuk autentikasi pengguna yang akan mengakses ke dalam jaringan *internet*. Karena manajemen user ini, akan memudahkan kita dalam memantau dan membuat jaringan *internet* yang aman. Cukup membuat satu akun pengguna disertai username dan password tersebut dapat digunakan atau mengakses jaringan *internet* yang telah di izinkan [24].

2.2.8. Hierarchical Token Bucket

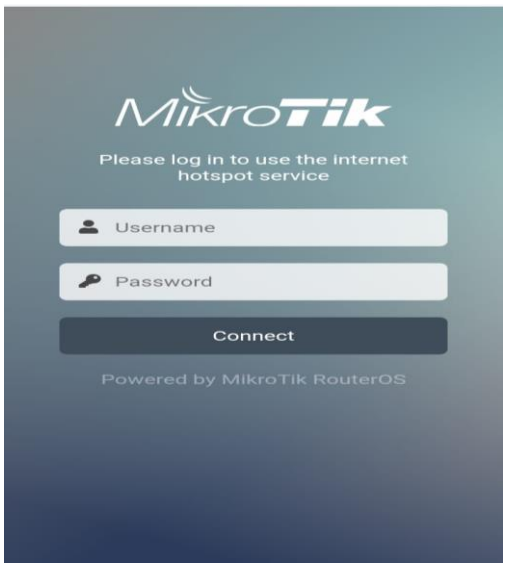
Hierarchical Token Bucket atau HTB merupakan sebuah metode manajemen *bandwidth* yang digunakan untuk mengatur jaringan *internet*. HTB ini bekerja dengan mengalokasikan *bandwidth* secara hierarkis berdasarkan kebutuhan pengguna. Memiliki keunggulan *bandwidth* yang tidak terpakai akan dibagi kembali sesuai dengan kebutuhan prioritas setiap pengguna dalam sebuah jaringan. Sehingga HTB dapat memberikan prioritas lebih kepada pengguna yang lebih penting. Oleh karena itu fungsi dari metode HTB yaitu untuk mengatur dan membatasi aliran data dalam jaringan dengan memprioritaskan penggunaan sumber daya berdasarkan aturan tertentu [17].



Gambar 2.2. Cara Kerja Hierarchical Token Bucket.

2.2.9. Captive Portal

Captive portal adalah halaman *login* sebelum mengakses jaringan *internet* yang berbentuk keamanan untuk melindungi jaringan dari pengguna yang tidak sah dan untuk memastikan bahwa pengguna telah diberikan izin untuk mengakses jaringan berupa *username* dan *password*. Dengan menggunakan *captive portal*, admin jaringan dapat membatasi akses ke jaringan hanya untuk pengguna yang terdaftar [25].



Gambar 2.3. Captive portal.

2.2.10. Firewall Filter

Firewall filter adalah pembatasan akses saat *user login* kemudian terhubung ke jaringan *internet* dimana pembatasan akses berupa *website-website* berbahaya yang bisa saja didalamnya terdapat *virus* yang dapat merugikan *user* dan perusahaan apabila terdapat data-data penting. Dapat dipahami kembali bahwa user yang telah *login* dan terhubung ke dalam jaringan *internet* PT. INKA Multi Solusi Service tidak akan bisa lagi mengakses *website-website* ilegal dan berbahaya menurut PT. IMSS (*website* yang menyediakan software bajakan) [7].

2.2.11. Router Mikrotik

Router *mikrotik* adalah hardware jaringan komputer yang dapat digunakan untuk menghubungkan jaringan yang sama atau berbeda. Router *mikrotik* merupakan perangkat jaringan yang dikembangkan oleh perusahaan *mikrotik* yang berfungsi sebagai alat untuk mengirimkan paket data via jaringan *internet* dan mengarahkan lalu lintas data agar dapat menuju tujuannya. Keunggulan router *mikrotik* memiliki kemampuan routing yang canggih, manajemen *bandwidth* yang kuat, didukung untuk protokol jaringan yang luas, dan memiliki kemampuan mengkonfigurasi sesuai dengan kebutuhan pengguna. Router *mikrotik* juga sering digunakan untuk membangun jaringan nirkabel dengan menggunakan fitur *access point* dan *bridge*. Beberapa seri router *mikrotik* yang populer yaitu *RouterBOARD* [26].

Router *mikrotik* didasarkan pada sistem operasi RouterOS yang dikembangkan oleh *mikrotik*. RouterOS adalah sebuah sistem operasi perangkat keras *RouterBOARD*. Dengan demikian,

memiliki semua fitur yang diperlukan untuk *filter firewall*, *manajemen bandwidth*, *captive portal*, manajemen *user*, *hotspot* dan banyak lagi [27].

Gambar 2.4. Router MikroTik RouterBoard.

2.2.12. Visual Studio Code

Visual studio code merupakan teks editor handal yang diciptakan oleh Microsoft buat sistem operasi multiplatfrom. Tersedia dan dapat digunakan untuk versi Linux, Mac, dan windows. Visual studio code ini support bahasa pemograman Node.js, JavaScript, dan Typescript serta bahasa pemograman lainnya (seperti C++, C#, Go, Java, Python, dst). Fitur-fitur yang disediakan visual studio code banyak, diantaranya Git Integration, Intellisense, Debugging, dan fitur lainnya. Fitur tersebut akan bertambah seiring pembaruan dari versi visual studio code nya, inilah yang membuat perbedaan visual studio code dengan teks editor lainnya. Teks editor ini bersifat open source, artinya dapat

melihat kode sumbernya dan dapat berkontribusi dalam pengembangannya. Hal ini membuat visual studio code menjadi favorit para developer aplikasi, Hal ini membuat visual studio code ini menjadi favorit para developer aplikasi karena para developer di masa mendatang dapat berpartisipasi dalam proses pengembangan visual studio code [28].

2.2.13. Bahasa Pemograman

Bahasa pemograman merupakan suatu intruksi yang digunakan untuk mengendalikan atau menginstruksi perintah-perintah sebuah komputer. Sekumpulan prosedur syntax dan semantic yang dipergunakan agar dapat menyediakan definisi kepada program komputer sehingga dikenal sebagai bahasa pemograman. Bahasa pemograman membuat seorang programmer untuk mengkomunikasikan logika, algoritma, dan prosedur keapda komputer agar dapat menjalankan tugas tertentu [29].

2.2.14. Bahasa Pemograman PhP

PhP (Hypertext Preprocessor) adalah suatu bahasa pemograman tinggi yang sering digunakan pada dokumen HTML dan untuk pengembangan aplikasi web dinamis. Sintaks PhP sama dengan bahasa C, Perl, dan Java, tetapi di bahasa PhP terdapat beberapa fungsi yang lebih detail. PhP digunakan untuk memungkinkan developer web yang dinamis dan bisa bekerja dengan otomatis [30].

2.2.15. Bahasa Pemograman CSS

CSS (Cascading Style Sheets) adalah bahasa pemograman yang digunakan untuk mengendalikan tampilan (style) dan presentasi pada halaman web. CSS digunakan untuk mengubah

atau mengatur style dari sebuah teks. Sehingga dengan menggunakan CSS dapat mengelola semua tampilan, seperti warna teks, besar font, tampilan layout, gambar background, posisi judul dan lainnya [31].

2.2.16. Bahasa Pemograman HTML

HTML (HyperText Markup Language) adalah bahasa standart yang digunakan untuk membangun halaman *website*. HTML sebuah bahasa yang digunakan untuk menggambarkan sebuah struktur serta isi semantik dari sebuah teks web. Sehingga bahasa pemograman HTML ini diibaratkan seperti kerangkanya [31].