BAB I PENDAHULUAN

1.1. LATAR BELAKANG

Tingginya permintaan jaringan *internet*, berbagai serangan bahkan ancaman, baik secara langsung maupun tidak langsung akan mempengaruhi aktifitas yang terjadi pada jaringan *internet* tersebut [1]. Keamanan jaringan *internet* merupakan mekanisme menangkal dan mengenali akses yang tidak sah. Langkah-langkah diperlukan untuk mencegah penyusup atau pengguna yang tidak sah mengakses sistem jaringan *internet* dan bagian-bagiannya [2].

Jumlah pengguna *internet* di Indonesia mencapai 78,19 persen di tahun 2023 atau 215.626.156 juta orang dari total seluruh penduduk Indonesia sebanyak 275.773.901 juta orang [3]. Dari banyaknya pengguna *internet* tersebut, beberapa masalah yang umum terjadi saat pengguna mengakses jaringan *internet* yaitu mengenai masalah manajemen *bandwidth*. Masalah pada manajemen *bandwidth* dapat terjadi ketika pengguna jaringan terlalu banyak *bandwidth* atau pembagian *bandwidth* tidak sesuai dengan kebutuhan pengguna sehingga dapat mempengaruhi kinerja jaringan dan koneksi *internet* menjadi lambat atau bahkan terputus [4]. Untuk menghindari masalah manajemen *bandwidth* tersebut yaitu menerapkan kebijakan penggunaan jaringan yang jelas dan teratur, dapat menggunakan *software* manajemen *bandwidth* untuk memantau dan mengontrol penggunaan *bandwidth* serta bisa menggunakan metode *Hierarchical Token Bucket* untuk memprioritaskan pengguna yang lebih penting serta mengatur pembatasan *bandwidth* untuk menghindari koneksi *internet* menjadi lambat [5].

Keamanan jaringan *internet* seringkali menjadi permasalahan yang muncul dalam penggunaan *internet*, salah satu masalah keamanan jaringan *internet* dapat terjadi ketika penggunaan *password* yang lemah atau penggunaan satu *password* yang sama untuk semua pengguna. Dengan penggunaan satu *password* untuk semua pengguna dapat menyebabkan mudahnya penetrasi jaringan *internet* oleh *user* yang tidak memiliki izin seperti *hacker.* Sehingga dapat mengakibatkan serangan *virus-virus* berbahaya

sehingga dapat merugikan pihak tertentu [6]. Demi menghindari masalah keamanan jairngan tersebut yaitu menerapkan *captive portal* ke sebuah jaringan *internet*. Tujuan *captive portal* untuk memungkinkan pengguna terhubung ke *internet* setelah memasukan informasi *login* atau memenuhi persyaratan tertentu. Sehingga admin dapat memantau siapa saja yang mengakses jaringan *internet* [6]. Kemudian masalah yang umum terjadi yaitu pembatasan akses *website*, pembatasan akses pada jaringan *internet* ini dilakukan untuk mengontrol akses pengguna ke *website* tertentu, terutama sumber *virus* jaringan. Dengan mengatur pembatasan akses, pengguna dapat menghindari hambatan dan meningkatkatkan produktivitas mereka dalam menggunakan jaringan *internet* [7].

PT. INKA Multi Solusi Servise (PT. IMSS) merupakan entitas anak perusahaan yang berasal dari PT. INKA Multi Solusi (PT. IMS), PT. IMS adalah perusahaan dibawah naungan PT. INKA (Persero). PT. INKA Multi Solusi Service juga perusahaan yang berbasis layanan jasa dibidang kereta api, transportasi dan infrastruktur [8]. Kantor PT. INKA Multi Solusi Service yang beralamat di Kota Madiun memiliki pegawai yang bekerja dengan komputer masing-masing serta kantor PT. INKA Multi Solusi Service berlangganan *internet* sebesar 150 Mbps yang dimilikinya. Tetapi jaringan *internet* di PT. INKA Multi Solusi Service memiliki permasalahan jaringan *internet* yang tidak optimal. Ini disebabkan oleh beban trafik pada jaringan yang berlebih dan alokasi *bandwidth* yang tidak tepat dengan kebutuhan sering juga menemukan pengguna yang tidak sah sehingga dapat menggunakan *internet* dan menggunakan *bandwidth* dengan seenaknya dan dapat merugikan pihak tertentu. Salah satu cara untuk solusinya yaitu menjalankan *Manajemen bandwidth* dengan memakai metode *Hierarchical Token Bucket*, karena memiliki kelebihan *bandwidth* yang tidak terpakai akan dibagi kembali sesuai dengan kebutuhan prioritas pada setiap pengguna dalam sebuah jaringan. Sehingga semua *bandwidth* bisa dimanfaatkan dengan baik dan optimal serta dapat memberikan prioritas lebih kepada pengguna yang lebih penting. Akan tetapi agar keamanan jaringan *internet* di PT. INKA Multi Solusi Service lebih

aman dan lebih baik dan melindungi dari serangan atau penyalahgunaan di dalam *internet*. Tidak dapat dipungkiri bahwa *internet* seringkali menjadi tempat terjadinya serangan dan penyebaran *virus* yang mengakibatkan banyak pengguna, perusahaan, dan pemerintah menjadi korban serangan dan menimbulkan kerugian yang signifikan. Maka dalam menjaga keamanan jaringan ini dilakukan *captive portal*, manajemen *bandwidth*, dan *firewall filter*, cara perlindungan jaringan dan penyeimbangan ini sering disebut sebagai *Firewall Filter* dan *Manajemen Bandwidth*.

Perangkat yang digunakan untuk mengembangkan sistem jaringan *internet* adalah *RouterBoard* dari *mikrotik*. *RouterBoard* adalah hardware dengan rangkaian router dan switch sehingga dapat digunakan untuk manajemen jaringan *internet* [9]. Metode operasi dasar *linux base* yang ditujukan menjadi *router* jaringan. Dibuat dengan tujuan memberikan kelancaran bagi penggunanya. Pengelolaannya dapat dijalankan melalui aplikasi *windows application* (*winbox*) yang terhubung dengan *system* jaringan *internet*. *Mikrotik* merupakan *system* operasi yang mencakup perangkat lunak yang diinstal pada komputer dengan demikian komputer berfungsi sebagai pusat kontrol jaringan, mengarahkan atau mengendalikan lalulintas antar jaringan [10].

Penelitian yang pernah dilakukan sebelumnya oleh Hadi Syahputra dan Romi Wijaya berjudul “Pembangunan Jaringan Hotspot Berbasis *Mikrotik* pada Kampung Tematik di Kecamatan Padang Utara”. Peneliti membuat jaringan *hotspot* berupa menara berbasis *mikrotik* sebagai lalu lintas jaringan dan telah berhasil diterapkan di Kampung Tematik Kecamatan Padang Utara [11]. Kemudian penelitian yang dilakukan oleh Tamsir Sriyadi dan Moh Rizki Alfyuddin dengan judul “Pemanfaatan Mikrotik Routerboard Untuk Optimasi *Bandwidth* Dan Keamanan Jaringan Di PT. Semen Baturaja (Persero) Tbk”. Peneliti telah menerapkan Manajemen *Bandwidth* memberikan *bandwidth* yang optimal pada jaringan *internet* PT. Semen Baturaja (Persero) Tbk Palembang karena bisa memecah *bandwidth* secara merata ke setiap ruangan, kemudian peneliti juga telah menerapkan *Radius Server* dapat menjadikan

keamanan pada jaringan sebagai *captive portal* sebelum menggunakan ISP yang tersedia, dan yang terakhir peneliti telah menerapkan sistem *Access Filter* tidak dapat menambah jumlah besar *Bandwidth* tetapi memfilter konten yang akan dibuka oleh *user*/karyawan [12].

Peristiwa serangan *siber ransomeware* Bank Syariah Indonesia hari senin tanggal 8 bulan mei tahun 2023 sempat membuat masyarakat Indonesia dan nasabah Bank Syariah Indonesia mengalami kepanikan. Karena data-data penting terkunci atau tidak dapat diakses serta tidak bisa melakukan transaksi di kantor cabang maupun melalui anjungan tunai mandiri (ATM). Sehingga Bank Syariah Indonesia dan nasabah Bank Syariah Indonesia mengalami kerugian yang besar [13].

Berdasarkan permasalahan di atas, perlu dilakukan penelitian dengan mengimplementasikan pengembangan sistem jaringan *internet* berbasis *router mikrotik* sehingga diharapkan dapat membantu kekurangan yang ada disistem jaringan *internet* PT. INKA Multi Solusi Service.

1.2. PERUMUSAN MASALAH

Berdasarkan latar belakang di atas, maka rumusan masalahnya adalah perlu dilakukan manajemen *user* dan keamanan menggunakan *captive portal*, manajemen *bandwidth* serta pembatasan akses terhadap *website* yang dianggap berbahaya sehingga dapat melengkapi kekurangan dan keamanan sistem jaringan *internet* yang ada di PT. INKA Multi Solusi Service.

1.3. PERTANYAAN PENELITIAN

1. Bagaimana cara implementasi pengembangan sistem jaringan *internet* PT. INKA Multi Solusi Service berbasis *router mikrotik?*
2. Bagaimana hasil analisis dari implementasi pengembangan sistem jaringan internet di PT. INKA Multi Solusi Service berbasis router *mikrotik*?
3. Apa saja alat dan bahan yang dibutuhkan dalam implementasi sistem jaringan *internet* PT. INKA Multi Solusi Service berbasis *router mikrotik?*

1.4. TUJUAN PENELITIAN

1. Mengoptimalkan dan meningkatkan keamanan sistem jaringan *internet* di PT. INKA Multi Solusi Service.
2. Pembagian *bandwidth* sesuai kebutuhan dan prioritas untuk memaksimalkan penggunaan *internet.*
3. Memblokir situs yang dapat mengganggu kinerja dan keamanan jaringan *internet.*

1.5. BATASAN MASALAH

1. Manajemen *user* dan keamanan menggunakan *captive portal* internal *mikrotik*.
2. Manajemen *bandwidth* menggunakan metode HTB (*Hierarchical Token Bucket*).
3. Pembatasan akses terhadap *website* yang dianggap berbahaya menurut PT. INKA Multi Solusi Service.
4. Pengembangan sistem jaringan *internet* ini menggunakan *router mikrotik*.

1.6. MANFAAT PENELITIAN

1. Bagi PT. INKA Multi Solusi Service

   Mampu melengkapi kekurangan sistem jaringan *internet* menjadi lebih seimbang dalam pembagian *bandwidth* dan lebih aman dengan menggunakan *router mikrotik.*

2. Bagi pembaca

   Menambah wawasan yang bisa digunakan untuk sumber informasi bagi penelitian lebih lanjut. Kontribusi nyata dalam pengembangan ilmu pengetahuan dan teknologi terutama implementasi dalam dunia industri teknologi informasi.