# IMPLEMENTASI SECURITY JARINGAN BERBASIS PROXY MENGGUNAKAN MIKROTIK OS UNTUK LOGIN DAN PEMBAGIAN BANDWIDTH

(studi kasus pada Politeknik Universitas Andalas)

**TUGAS AKHIR**


**Oleh :**

**NOFRIALDI**

**Bp.06093033**


**PROGRAM STUDI TEKNIK KOMPUTER**

**JURUSAN TEKNOLOGI INFORMASI**

**POLITEKNIK UNIVERSITAS ANDALAS**

**PADANG**

**2009**

## ABSTRAKSI

Seiring dengan semakin meningkatnya pengguna *internet*, semakin banyak pula pihak-pihak yang tidak bertanggung jawab yang ingin memanfaatkan jaringan tersebut dengan tujuan yang tidak baik. Untuk itu perlu diciptakan suatu sistem yang dapat mengamankan *internet* tersebut. Metode yang digunakan adalah dengan penambahan halaman verifikasi untuk mengakses *internet*.

Proses pembangunan halaman verifikasi ini menggunakan *mikrotik Operating System* (OS). Konfigurasi yang dilakukan hanya pada bagian *radius* dan *hotspot* yang sudah ada pada *mikrotik* OS.

Dengan penggunaan sistem verifikasi ini akan membuat *internet* lebih aman dari pihak-pihak yang tidak bertanggung jawab. Disamping itu penggunaan halaman verifikasi ini juga akan membuat *internet* lebih stabil karena kapasitas akses *user* jaringannya dibatasi.



Kata kunci : *Radius, Hotspot, Mikrotik Operating System*

# BAB I

# PENDAHULUAN

## 1.Latar Belakang

Jaringan merupakan suatu perangkat yang sudah tidak bisa dipisahkan lagi dari komputer. Seiring dengan semakin pesatnya pertumbuhan pengguna komputer di seluruh dunia juga berakibat pada kebutuhan jaringan yang semakin meningkat. Jaringan itu sendiri berguna untuk berbagai hal, mulai dari sekedar pertukaran data sampai penggunaan suatu perangkat secara bersamaan. Namun seiring dengan perkembangan komputer dan jaringan, pengerusakan data dalam jaringan juga meningkat.

Untuk menciptakan keamanan pada jaringan tersebut maka diperlukan teknik-teknik yang dapat digunakan untuk memimalkan pengerusakan yang terjadi. Hal ini dapat diminimalkan namun tidak dapat dijamin aman 100% karena jaringan menggunakan hukum 0 dan 1 sehingga hampir dapat dipastikan bagaimanapun jenis jaringan tersebut pasti bisa disusupi *hacker*. Namun dengan adanya pemberian *security* setidaknya dapat memperlama pekerjaan pengerusakan yang dilakukan *hacker* pada suatu jaringan, dan disamping itu *network administrator* juga dapat mengambil tindakan yang tepat. Tindakan ini mulai dari menunggu sampai pengerusakan yang dilakukan *hacker* berhenti dengan sendirinya, ataupun dengan cara mengeluarkan *hacker* tersebut dari jaringan, namun jika kegiatan yang dilakukan *hacker* seperti merusak data belum bisa dihentikan, maka dilakukan isolasi server atau pemutusan hubungan server dengan jaringan.

*Proxy* merupakan suatu perangkat keamanan jaringan yang dapat digunakan untuk membatasi hak akses *user* dalam suatu jaringan. Hal ini digunakan untuk mengamankan data yang tidak boleh diakses *user* secara bebas.

Disamping *proxy*, radius juga sangat berguna dalam keamanan jaringan. Hal ini dikarenakan radius dapat digunakan untuk penyaringan atau pembatasan user yang hendak mengakses suatu jaringan. Langkah yang digunakan dalam penggunaan radius sangat sederhana, dimulai dengan pemberian *user name* dan *password* yang telah diatur sebelumnya oleh *network administrator*. Sedangkan untuk perusahaan-perusahaan besar yang menggunakan banyak komputer biasanya menggunakan metode penyaringan alamat fisik atau MAC *Address* dari sebuah perangkat jaringan yang terdapat pada user, perangkat yang disaring MAC *Addressnya* adalah kartu jaringan yang digunakan user untuk terhubung ke jaringan.

Untuk perangkat pendukung dalam pembagian *bandwidth* juga digunakan *router*, dalam penggunaannya router akan memberikan peranan dalam efisiensi waktu dalam pemilihan jaringan, hal ini terjadi karena *router* memiliki kemampuan mencari jalan terbaik pada suatu jaringan. Disamping itu *router* juga sering digunakan sebagai keamanan tingkat lanjut dalam suatu jaringan.

Mikrotik adalah salah satu perangkat *router* yang paling baik saat ini. Hal ini diputuskan berdasarkan kualitas dan sejarah penggunaannya di banyak perusahaan besar yang sangat baik dan jarang sekali mengalami gangguan. Mikrotik sama dengan *router* pada umumnya, memiliki suatu metode untuk meminimalisir *hacker* melalui *ip table* yang dimilikinya. *Ip table* sendiri berfungsi sebagai keamanan tingkat dua dalam suatu jaringan *wireless*, hal ini karena keamanan tingkat satunya terletak pada

*accsess point* melalui enskripsi yang dimilikinya, salah satu model enskripsi pada *accesss point* adalah WPA (*Wi-Fi Protected Access)*. Mikrotik juga mendukung sistem pembagian bandwidth, sehingga dapat memberikan hak akses lebih kepada *user* yang lebih diprioritaskan.

Berdasarkan kelengkapan fitur yang dimiliki oleh mikrotik menyebabkan banyaknya penggunaan perangkat ini pada perusahaan-perusahaan skala menengah sampai skala besar. Mikrotik disamping digunakan sebagai *router* juga sangat handal dijadikan sebagai proxy server. Hal ini dikarenakan fasilitas *security* yang dimilikinya sudah terbukti kekuatannya di perusahaan-perusahaan besar.

Berdasarkan atas informasi, penulis membuat sebuah implementasi pembagian *user* berdasarkan data yang telah ada di *database*, dan berdasarkan data tersebut, akan ditentukan berapa bandwidth yang boleh digunakan *user*,yang dibentuk kedalam Tugas Akhir untuk menyelesaikan studi pada program diploma di Politeknik Universitas Andalas dengan judul "Implementasi Security Jaringan Berbasis *Proxy* Menggunakan *Mikrotik OS* Untuk *Login* Dan Pembagian Bandwidth".

## 1.2 Rumusan Masalah

Adapun rumusan masalah dari penulisan ini adalah :

1. Apa saja langkah-langkah yang dilakukan untuk melakukan *subnetting router* agar dapat membedakan bandwidth yang diberikan kepada *user* sesuai dengan data yang ada pada radius ?
2. Bagaimana cara instalasi dan konfigurasi radius untuk membedakan *user* normal dan *user* prioritas ?

3. Bagaimana cara memberikan enskripsi pada *access point* sebagai level keamanan tingkat satu ?
4. Bagaimana cara pengkonfigurasian *ip table* pada *mikrotik* sehingga bisa digunakan sebagai level keamanan tingkat dua ?

## 1.3 Tujuan

Adapun Tujuan dari penulisan ini adalah untuk memudahkan semua yang berkaitan dengan jaringan tersebut, baik *user* ataupun *administrator*.

### 1.3.1 Umum

Adapun tujuan umum dari penulisan ini adalah :

1. Memberikan kenyamanan pada *user*, karena kecepatan yang didapat dalam mengakses jaringan stabil.
2. Mengamankan jaringan dari serangan *hacker* karena semua aktifitas *user* dibatasi beberapa level keamanan.

### 1.3.2 Khusus

Adapun tujuan khusus dari penulisan ini adalah sebagai berikut :

1. Bagaimana mempermudah *network administrator* dalam pemantauan jaringan dan bagaimana memperkuat jaringan atas kemungkinan penyusupan yang terjadi.
2. Bagaimana membuat *server* tidak *down* dengan mengurangi aktifitas *download* yang berlebihan di siang hari.

# BAB V

# PENUTUP

## 5.1 Kesimpulan

Dari percobaan sistem yang telah dibuat maka dapat diambil kesimpulan :

1. Sistem keamanan tingkat satu pada *access point* perlu diaktifkan pada setiap jaringan yang tidak digunakan untuk jaringan publik, hal ini akan membuat jaringan lebih aman dan tidak mudah disusupi pihak tidak bertanggung jawab.
2. Penggunaan pembagian *bandwidth* menggunakan halaman *login* sangat menguntungkan, hal ini dikarenakan hanya *user* prioritas yang akan mendapatkan kecepatan lebih, namun tetap diberikan batasan sehingga kestabilan koncktifitas pada jaringan dapat terjaga.
3. Kegiatan *download* berlebihan yang biasanya terjadi sudah dapat dikurangi dengan adanya pembatasan *upload* dan *download*.
4. Dengan menngunakan system ini kegiatan *user* dapat dipantau, sehingga jika terjadi sesuatu yang mencurigakan dalam jaringan, bisa langsung diketahui siapa pelakunya melalui IP *address* dan MAC *address* yang terdeteksi oleh sistem.
5. Yang paling penting diperhatikan pada *system* ini adalah *IP address* yang digunakan, hal ini dikarenakan jika terjadi konflik *IP address* maka akan mempengaruhi kinerja *mikrotik* secara kescluruhan.
6. Hal Kecil yang paling sering mengganggu dalam pembuatan sistem ini adalah kartu jaringan yang perlu di periksa ulang. Banyak kartu jaringan yang dapat terdeteksi oleh sistem namun tidak dapat digunakan karena rusak.

# DAFTAR PUSTAKA


Pribadi, Harijianto. **Firewall melindungi DDOS menggunakan LINUX+MIKROTIK**. Yogyakarta : Andi, 2007.

Heriadi, Dodi. **Jaringan WI-FI**. Yogyakarta : Andi, 2008.

Madcoms. **Membangun Sistem Jaringan Komputer**. Yogyakarta : Andi, 2009.

Rafudin, Rahmat. **Membangun Firewall dan Trafic Filtering Berbasis Cisco**. Yogyakarta : Andi, 2008.

S'to. **Wireless Kung Fu**. Yogyakarta : Jasakom, 2007.