# IMPLEMENTASI PENANGANAN SERANGAN *MAC-CLONE* PADA *HOTSPOT* MIKROTIK DI STMIK PRADNYA PARAMITA MALANG (STUDI KASUS: STMIK PRADNYA PARAMITAMALANG)

**Santi Dwi Ratnasari[1)], Dwi Safiroh Utsalina[2)]**
[1]Program Studi Teknik Informatika, STMIK Pradnya Paramita Malang
Email : santi26.ratnasari@gmail.com
[2]Program Studi Sistem Informasi, STMIK Pradnya Paramita Malang
Email : utsalina@gmail.com

***Abstract***

*One of the facilities that is needed is a network agency. In educational institutions such as Colleges and universities are needed to look for references as well as add insight. The technology used is one that is technology hotspot. Currently there are many hotspot technology is applied to the High School and College. However, the hotspot network mikrotik used in STMIK Pradnya Paramita Malang still experienced many problems in network security. Attacks are frequent and intrusive security network that attacks Mac Clone. Disrupt and complicate the issue of employees as well as students who have access rights legally due access rights are duplicated by users who are not responsible. Therefore, to overcome these problems built a network security by firewall settings that the filter rule and NAT. Based on test results concluded that in building a network security RouterOS hotspot using 5.18 to leave the setting on the firewall, can address the existing Mac Clone attack on STMIK Pradnya Paramita Malang.*

***Keywords*: *Firewall, Hotspot, Mac Clone, Mikrotik RouterOS 5.18.***

## 1. PENDAHULUAN

STMIK Pradnya Paramita merupakan Sekolah Tinggi yang berdiri sejak 26 Juli 2000 di Malang. Keamanan jaringan merupakan yang penting untuk diperhatikan oleh sebuah Sekolah Tinggi. Oleh karena itu, diperlukan penanganan jaringan dari berbagai serangan, salah satunya yaitu serangan MAC-*clone.* Adanya penanganan serangan MAC-*clone* dapat mengembalikan hak *autoritas* pemilik *user,* agar *user* yang dimiliki tidak mudah di duplikat oleh pengguna lain.

Serangan MAC-*clone* merupakan serangan yang sering terjadi pada mikrotik, dimana satu *user* dapat digunakan untuk login lebih dari satu orang atau dapat disebut duplikasi. Jika masalah MAC-*clone* tidak segera ditangani maka akan berdampak negatif pada sistem keamanan *user,* sehingga *autoritas* pemilik *user* sudah tidak menjadi bahan pertimbangan. Berdasarkan data yang didapat, dalam satu bulan bisa terjadi serangan sampai tiga puluh kali bahkan bisa lebih dari itu. Hal ini sangat merugikan pemilik *user,* terutama dalam segi *bandwidth,* koneksi, serta pada kecepatan akses *internet.* Jika serangan MAC-*clone* tidak segera ditangani hal tersebut akan sangat mengganggu aktivitas *user,* memang tidak berdampak pada *server,* melainkan berdampak pada *user.* Secara tidak langsung dampak negatif akibat serangan MAC-*clone* dapat dirasakan, seperti tidak lancarnya proses pencarian pada *browser* dan proses pencarian yang lain sehingga menghambat kegiatan belajar mengajar disaat menggunakan akses *wifi* yang tersedia.

Sistem keamanan jaringan yang terbentuk pada mikrotik yang digunakan saat ini, belum mendukung penanganan serangan MAC-*clone.* Oleh karena itu, dibutuhkan *setting* tambahan misalnya dengan memanfaatkan *firewall,* agar dapat menyaring lalu lintas dengan menggunakan alamat IP, MAC *Address,* nomor port dan protokol. Sehingga hanya lalu lintas resmi yang diperbolehkan untuk terus berjalan, *firewall* juga memiliki kemampuan untuk mem*filter* paket lalu lintas yang masuk ke dalam jaringan lokal. Jika pemanfaatan *firewall* berhasil dilakukan untuk menangani masalah serangan MAC-*clone,* maka nantinya dapat digunakan oleh *user* untuk keamanannya agar tidak mudah di duplikasi oleh orang lain. Pada penelitian kali ini, peneliti menggunakan *settingan firewall* yaitu pada *filter rule* nya dan juga NAT. Penggunaan *settingan* tersebut dapat mempermudah untuk penyaringan lalu lintas data *login* dengan

menggunakan pemblokkan pada MAC *Address.*

Berdasarkan latar belakang yang telah dijelaskan maka peneliti mengambil judul "Implementasi Penanganan Serangan MAC-*Clone* Pada *Hotspot* Mikrotik Di STMIK Pradnya Paramita Malang".

Berdasarkan latar belakang yang telah dipaparkan, maka dapat dirumuskan permasalahan sebagai berikut: Bagaimana cara mengatasi serangan MAC-clone pada jaringan mikrotik STMIK Pradnya Paramita Malang?

Permasalahan yang dibahas dalam penelitian ini, di batasi pada:

a. Perancangan topologi jaringan menggunakan simulator Cisco Packet Tracer.
b. Alat yang digunakan yaitu mikrotik RouterOS versi 5.18.
c. Pengintergrasian mikrotik dengan memanfaatkan *VirtualBox* dan *winbox*.
d. Jaringan yang diterapkan adalah jaringan lokal STMIK Pradnya Paramita Malang.
e. Keamanan yang digunakan yaitu dengan menggunakan settingan pada *firewall* yaitu pada *filter rules* dan NAT.

Adapun tujuan penelitian yang dilakukan adalah : Terciptanya sistem keamanan pada mikrotik untuk mengatasi serangan MAC-*clone* pada kampus STMIK Pradnya Paramita Malang.

Adapun manfaat yang dapat diperoleh dari penelitian ini adalah sebagai berikut:

a. Bagi Tempat Penelitian (STMIK Pradnya Paramita Malang)
   Membantu menangani serangan MAC-*clone* untuk mengembalikan autoritas *user.*
b. Bagi Pengembangan Ilmu
   Membantu peneliti selanjutnya membangun sistem keamanan jaringan tersebut (sebagai referensi).

## 2. LANDASAN TEORI

### 2.1 Jaringan Komputer

Jaringan komputer adalah sebuah system yang terdiri atas beberapa unit komputer yang didesain sedemikian rupa sebagaimana tujuan utamanya yakni untuk dapat be, drbabi sumber daya (*CPU, printer, scanner, plotter, hardisk*, dan sebagainya), berkomunikasi (pesan instan, surel), dan dapat mengakses informasi (situs web). Menurut pembagiannya, jaaringan komputer dapat dibedakan menjadi dua jenis, yakni jaringan terdistribusi dan jaringan tersentral (Madcoms, 2015:2).

### 2.2 *MAC-Clone (MAC Address Clone)*

MAC (Mac Access Control) address adalah alamat sebuah hardware atau alamat fisik yang secara unik mengidentifikasi setiap komputer atau alat yang terhubung dalam jaringan, MAC *address* juga sering disebut *physical/hardware address.* (Jubilee Enterprise, 2009:86).

Berikut adalah beberapa fungsi dari MAC *address* :

a. Memberikan kontrol terhadap alat apa saja yang bisa terkoneksi dengan *router*.
*b.* Membatasu akses berdasarkan MAC *access lists* (ACLs) yang tersimpan dan didistribusikan dalam hampir setiap jenis *router.*
*c.* Memiliki kmampuan penyaringan akses ke dalam sebuah komputer menggunakan daftar perijinan *(permissions list)* yang dibuatkan berdasarkan MAC *address.*

MAC *clone* merupakan suatu tindakan pembobolan, duplikasi *(cloning)* pada alamat sebuah hardware atau alamat fisik pada komputer agar memiliki MAC *address* yang sama tujuannya agar dapat dengan mudah masuk ke dalam jaringan tanpa melakukan perijinan dari *administrator* terlebih dahulu. (Jubilee Enterprise, 2009:86).

### 2.3 *Firewall*

*Firewall* atau dinding api adalah sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk dapat melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. Pada dasarnya sebuah firewall dipasang pada sebuah router yang berjalan pada *gateway* antara jaringan lokal dengan jaringan Internet (Wahana Komputer, 2014:72).

#### a) Fungsi *Firewall*

Menurut Wahana Komputer (2014:72), *Firewall* berperan dalam melindungi jaringan dari serangan yang berasal dari jaringan luar. *Firewall* mengimplementasikan paket *filtering*. Dengan demikian, *firewall*

menyediakan fungsi kemanan yang digunakan untuk mengelola aliran data ke , dari, dan melalui router. Berikut fungsi – fungsi *firewall* secara umum:

1. Mengontrol dan mengawasi paket data yang mengalir di jaringan.

*Firewall* harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi *firewall*. *Firewall* harus dapat melakukan pemeriksaan terhadap paket data yang akan melewati jaringan private. Beberapa kriteria yang dilakukan *firewall* apakah memperbolehkan paket data lewati atau tidak, antara lain:

   a. Alamat IP dari komputer sumber
   b. Port TCP/UDP sumber dari sumber
   c. Alamat IP dari komputer tujuan
   d. Port TCP/UDP tujuan data pada komputer tujuan
   e. Informasi dari *header* yang disimpan dalam paket data

2. Melakukan autentifikasi terhadap akses.
3. Aplikasi Proxy

*Firewall* mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

4. Mencatat semua kejadian di jaringan

Mencatat setiap transaksi kejadian yang terjadi di *firewal*l. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

### 2.4 *Hotspot*

Menurut Iwan Sofana (2008:355), *hotspot* adalah tempat khusus yang disediakan untuk mengakses *internet* mengunakan peralatan *Wi-fi.* Umumnya layanan *hotspot* bersifat gratis. Dengan berbekal laptop atau PDA maka koneksi *internet* dapat dilakukan secara cuma-cuma. Biasanya pengguna terlebih dulu harus melakukan registrasi kepenyedia layanan *hotspot* untuk mendapatkan *login* dan *password.* Kemudian pengguna dapat mencari area *hotspot*, seperti pusat perbelanjaan, kafe, hotel, kampus, sekolahan, bandara udara, dan tempat-tempat umum lainnya.

Proses otentikasi dilakukan ketika *browser* diaktifkan. Untuk membuat hotspot dibutuhkan alat seperti *accesss point (AP). Access point* bisa dianalogikan dengan *hub* dan *repiter* pada (*wired LAN*). *Access point* dapat menerima dan meneruskan sinyal dari berbagai peralatan *WIFI*. *Access point* juga dapat menggabangkan jaringan *wireless* dengan *wired* dan dapat memperbesar jangkauan WLAN.

Ada beberapa kelebihan hotspot diantaranya ;

- Banyaknya disediakannya koneksi di tempat umum, seperti café, lobi hotel, restoran, executive lounge bandara dll.
- User bisa bekerja secara mobile tanpa harus mencari plug koneksi
- Membuang kerumitan kabel dan membuat perusahaan bisa konsentrasi ke business processnya
- Transfer data bisa mencapai 11 mbps dengan troughput yang besar dan tergantung standart yang digunakan
- Kompabilitas dengan banyak devices yang sudah terdapat Wi-Fi enabled
- Trend dan branding

### 2.5 Mikrotik

Mikrotik merupakan sebuah perusahaan yang bergerak di bidang produksi perangkat keras (*Hardware*) dan perangkat lunak (*Sofware*) yang berhubungan dengan sistem jaringan komputer yang berkantor pusat di Latvia, bersebelahan di Rusia. Mikrotik didirikan pada tahun 1995 untuk mengembangkan router dan sistem ISP (*Internet Service Provider*) nirkabel.

Mikrotik adalah router yang dibangun dari sistem operasi Linux, hanya saja dimodifikasi sedemikian rupa sehingga fungsinya spesifik ke arah routing dan fungsi jaringan. Alat ini dapat digunakan untuk routing static, routing dinamik, *hotspot*, *firewall*, VPN, DHCP Server, DNS *cache*, dan *web proxy* (Ino Irvantino 2014:1).

## 3. METODE PENELITIAN

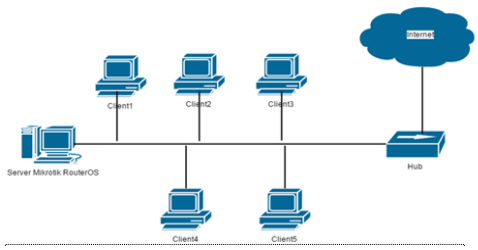
### 3.1 Analisis Masalah

#### 3.1.1 Sistem jaringan yang sudah ada

STMIK Pradnya Paramita merupakan sebuah Sekolah Tinggi berbasis komputer di Malang yang memiliki jaringan cukup besar. Konsep pengaksesan internet di mulai dari jaringan luar yang langsung terhubung dengan internet. Internet di hubungkan oleh *RouterPC.* Jaringan di STMIK Pradnya Paramita masih belum terdapat pengamanan untuk menangani serangan MAC-*clone,* yang mana serangan tersebut dapat menduplikasi user yang sudah terdaftar agar bisa akses di internet. Kampus STMIK Pradnya Paramita

menggunakan mikrotik *RouterOS* versi 15.8. Selain itu, STMIK Pradnya Paramita menggunakan ISP Indihome dengan *bandwidth* sebesar 100 *Mbps* yang digunakan untuk semua pengguna di kampus STMIK Pradnya Paramita Malang. Topologi yang digunakan adalah topologi *bus*.

Topologi jaringannya terlihat pada gambar 3.1



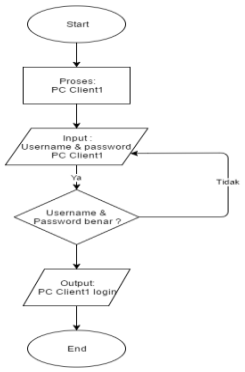

:

Gambar 3.1 Topologi Jaringan Kampus Stimata

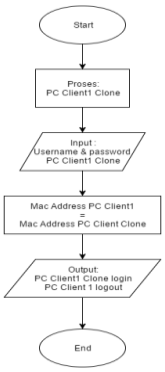
### 3.1.2 Analisis permasalahan yang ada

Sistem jaringan yang ada di STMIK Pradnya Paramita belum menggunakan pengamanan terhadap serangan MAC-*clone* sehingga user yang sudah terdaftar dapat digandakan dengan mudah, hal ini yang membuat pemilik *user* tidak nyaman dalam melakukan kinerja dikarenakan hak *autoritas* akses jaringan (*ISP)* yang mereka gunakan diambil alih oleh *user* yang tidak bertanggung jawab. Pemilik *user* tidak mengetahui bahwa *username*nya telah diduplikasi oleh orang lain. Hal ini juga dikarenakan sistem keamanan jaringan yang ada pada STMIK Pradnya Paramita masih belum bisa menangani masalah tersebut dikarenakan belum di*setting* keamanannya secara menyeluruh. Dalam penulisan ini peneliti melakukan percobaan dengan melakukan pembangunan *hotspot* serta melakukan monitoring pada ARP List agar mengetahui siapa saja yang *login* ke dalam jaringan. Selain itu, peneliti juga menambahkan pengembangan yang akan dilakukan di STMIK Pradnya Paramita dengan menambahkan *settingan* pada *hotspot* serta *firewall*, yang akan membantu pemilik *user* mendapatkan kembali hak *autoritas*nya.

Berikut adalah flowchart yang menjelaskan alur permasalahan yang ada pada gambar 3.2 dan gambar 3.3 :




Gambar 3.2 Proses *Login* PC *Client1*




Gambar 3.3 Proses *Login* PC *Client1 Clone* dan Permasalahan yang Terjadi

Pada flowchart ini, sebelum dipasang keamanan untuk penanganan *MAC-Clone* mengambil contoh PC *Client1* untuk login terlebih dahulu, PC *Client1* berhasil login. Selanjutnya dilakukan pengujian terhadap PC *Client1 Clone* untuk login dengan menggunakan *username* dan *password* yang sama dengan *PC Client1* dengan kondisi memiliki *MAC Address* yang sama. Hasilnya *PC Client1 Clone* berhasil login dan PC *Client1 logout* secara otomatis, dengan kata lain hak akses PC *Client1* diambil alih oleh PC *Client1 Clone.*

## 3.2 Solusi Masalah

Meskipun telah menggunakan jaringan melalui *ISP* tetapi jika penanganan MAC-*clone* belum ada, itu akan membuat aktivitas di STMIK Pradnya Paramita tidak nyaman. Hal tersebut dikarenakan sering terjadi MAC-*cloning* sehingga ketika melakukan *browsing* tiba-tiba saja tidak dapat terkoneksi seperti awalnya. Maka untuk mengatasi permasalahan tersebut perlu diadakan implementasi pengamanan dari serangan MAC-*clone* sehingga dapat meminimalisir terjadinya *cloning* MAC *Address* yang diambil oleh *user* yang tidak meminta ijin (illegal) yang mengakibatkan terjadinya masalah pada aktivitas di STMIK Pradnya Paramita, sebagai contoh : waktu kegiatan belajar mengajar yang membutuhkan koneksi internet, tetapi ketika ada *user* yang sudah *login* tiba – tiba saja tidak dapat terkoneksi dengan internet dan jaringan internet tidak cepat (lemot) sehingga waktu mengerjakan soal habis hanya untuk menunggu terkoneksi kembali serta menunggu koneksi internet yang tidak lancar,

disitu salah satu kerugian bagi pengguna jaringan di STMIK Pradnya Paramita. Dalam pengembangan ini penulis juga menambahkan pengembangan yang akan dilakukan di STMIK Pradnya Paramita yaitu dengan menambahkan settingan *firewall* yang akan mempermudah *user* dalam melakukan kegiatan serta mengembalikan hak *autoritas* pengguna jaringan di STMIK Pradnya Paramita.

### 3.3 Metode Pengumpulan Data

#### 3.3.1 Wawancara

Tahap ini dilakukan wawancara kepada karyawan dengan jabatan sebagai admin jaringan, serta kepada mahasiswa di STMIK Pradnya Paramita untuk mengetahui sistem jaringan yang telah ada serta permasalahan yang terjadi. Berikut hasil wawancaranya:

a. Bagaimana menurut anda sistem jaringan yang sedang berjalan sekarang di STMIK Pradnya Paramita?
   Jawab: Ketika saya melakukan *login* awalnya sudah bisa, tapi beberapa saat kemudian koneksi saya terputus, kemungkinan besar MAC *address* saya sudah ada yang duplikasi.
b. Apa yang sering dikeluhkan *user* tentang jaringan di STMIK Pradnya Paramita?
   Jawab: Kebanyakan tentang Internet yang lambat, tidak stabil, dan *logout* secara tiba-tiba.
c. Apa penyebabnya Internet lambat dan tidak stabil?
   Jawab: Banyak faktor yang mempengaruhi Internet lambat dan kadang tidak stabil. Salah satunya adalah banyak *user* yang tidak terdaftar dengan mudah dapat melakukan akses internet, bisa dikatakan adanya penduplikasian *user*.
d. Bagaimana teknisi jaringan di sana mengatasi atau meminimalis keadaan tersebut?
   Jawab: Sudah diimplementasikan beberapa cara untuk mengatasinya, namun masih belum mendapatkan hasil yang sesuai dengan yang diharapkan.
e. Apa masalah yang diakibatkan oleh ketidak stabilan internet?
   Jawab: masalahnya, disaat kegiatan belajar mengajar yang membutuhkan koneksi internet akan menghambat prosesnya, serta pengguna akan jenuh jika kondisi internet masih belum stabil. Selain itu, lama-lama pengguna akan beralih untuk menggunakan koneksi lain, dikarenakan hak *autoritas* pengguna sudah tidak menjadi bahan pertimbangan lagi
f. Apa harapan Anda ke depan buat internet di STMIK Pradnya Paramita?
   Jawab: Saya berharap hak *autoritas* pengguna diutamakan, sehingga tidak merugikan pengguna aslinya agar mempermudah dalam proses *browsing.*

#### 3.3.2 Observasi

Tahap ini dilakukan pengamatan langsung ke tempat penelitian dan untuk mengetahui aktivitas yang dilakukan pada ruangan STMIK Pradnya Paramita. Observasi ini dilaksanakan pada:

Hari/Tanggal : Rabu, 5 Oktober 2016
Waktu : Pukul 18.00 – 20.00 WIB
Tempat : Ruangan STMIK Pradnya Paramita.

Tujuan dari observasi pada ruangan *server* jaringan di STMIK Pradnya Paramita adalah untuk mengetahui situasi dan kondisi dari sistem jaringan yang sedang berjalan serta teknologi yang digunakan untuk mendukung sistem jaringan di STMIK Pradnya Paramita.

#### 3.3.3 Studi Pustaka

Tahap ini dilakukan untuk mempelajari teori-teori dari buku, artikel, dan jurnal yang berhubungan dengan penelitian sebagai sumber studi pustaka dan pendalaman teori dalam pengembangan sistem jaringan yang dibuat. Pendalaman teori yang di pelajari adalah tentang dasar-dasar jaringan, metode yang digunakan dalam *manajemen bandwidth*, keamanan internet dan penanganan *Mac-clone*, pemanfaatan mikrotik *RouterOS* serta teknologi *software* dan *hardware* yang berhubungan dengan sistem jaringan.

#### 3.3.4 Hasil Pengumpulan Data

Dari hasil pengumpulan data melalui tahap wawancara dan observasi dapat dibuat hasil wawancara dan observasi sepert tabel 3.1

Tabel 3.1 Hasil Dari Wawancara dan Observasi Spesikasi *Hardware*

| Analisis Teknologi yang digunakan | Hasil Analisis |
|---|---|
| Jenis Layanan | *LAN*, Internet, *hotspot*. |

| Analisis Teknologi yang digunakan | Hasil Analisis |
|---|---|
| Skalabilitas | Luas, terdapat kurang lebih 100 *user*. |
| *Explandable* | Dapat di perluas sesuai kebutuhan. |
| Media Transmisi | Kabel dan *Nirkabel*. |
| Kondisi gedung dan ruangan | Jaringan dalam satu ruangan, tetapi dilakukan pengembangan diseluruh area kampus. |
| *Bandwith* | - Indihome *bandwith* 100 *Mbps.*<br>- Menggunakan Manajemen *Bandwith Queue Tree.* |
| Spesifikasi *Hardware* | - IBM x3250 m5<br>- *Processor* Intel Pentium 4 G3420 3,2GHz,<br>- *Memory* 1 x 4Gb up to 32Gb Max,<br>- Power Supply 300W 80+ *certified*,<br>- *Storage* 500GB 7,2k SS 3,5in SATA. |

Tabel 3.2 Hasil Dari Wawancara dan Observasi

Spesikasi *Software*

| Analisis Teknologi yang digunakan | Hasil Analisis |
|---|---|
| Spesifikasi *Sofware* | 1. Sistem Operasi Windows xp untuk *Client.*<br>*2. Winbox*<br>*3. IDM* |
| *Monitoring* Sistem | Dilakukan di ruangan administrator jaringan |
| Keamanan Jaringan | - Ada, tapi belum maksimal |
| Sumber Daya Manusia | Memiliki SDM di bidang IT jaringan |

### 3.4 Perancangan Sistem Jaringan

Tahap perancangan sistem jaringan bertujuan untuk memberikan solusi untuk mengatasi sistem permasalahan yang ada. Dari data yang telah didapatkan dari tahap analisis dan hasilnya, maka dapat di rancang struktur jaringan yang menjelaskan gambaran umum alur proses dari sistem perancangan jaringan yang dibuat di STMIK Pradnya Paramita.

Perancangan system jaringan dalam membangun system keamanan jaringan dengan melakukan *setting* pada *firewall* menggunakan metode *Network Development Life Cycle* (NDLC), memiliki konsep perancangan yang sederhana dan mudah dipahami. Dengan metode NDLC diharapkan keamanan internet yang dilakukan *setting*an pada *firewall* yang akan dibangun dapat membantu pihak STMIK Pradnya Paramita yang selama ini mengalami permasalahan saat menggunakan jaringan yaitu seringnya tiba-tiba *logout* dengan sendirinya. Tahapan untuk model pengembangan NDLC :

1. *Analysis*

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya adalah wawancara, survey langsung ke lapangan.

2. *Design*

Dari data-data yang didapatkan sebelumnya, tahap *design* ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain bisa berupa desain struktur topologi yang akan memberikan gambaran jelas tentang proyek yang akan dibangun.

3. *Simulation* Prototyping

Beberapa pekerja jaringan akan membuat dalam bentuk simulasi dengan bantuan *tools* khusus di bidang *network* seperti GNS3, Packet Tracer, Netsim, dan sebagainya. Hal ini dimaksudkan untuk melihat kinerja awal dari jaringan yang akan dibangun dan sebagai bahan presentasi dan sharing dengan *team work* lainnya.

4. *Implementation*

Pada tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi pekerja jaringan akan menerapkan semua yang telah direncanakan dan didesain sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil atau gagalnya proyek yang akan dibangun dan ditahap inilah *team work* akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis.

5. *Monitoring*

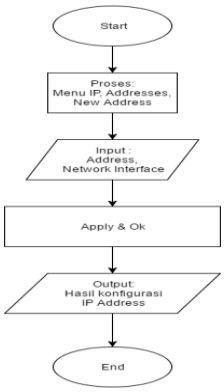
Setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring.

6. *Management*

Pada level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (*policy*). Kebijakan perlu dibuat untuk membuat atau mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga.

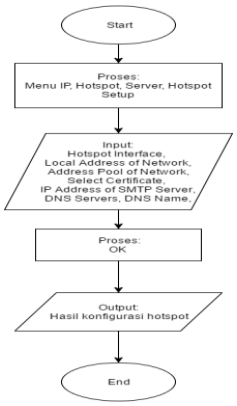
### 3.5.1 Perancangan *Hotspot* pada Mikrotik *RouterOS 5.18*

Tahap ini dilakukan perancangan *hotspot*, yang digunakan untuk proses untuk bisa melakukan percobaan untuk *login* baik sebelum dan sesudah dibangunnya keamanan pada jaringan. Sebelum dilakukan perancangan *hotspot* terlebih dahulu konfigurasi IP *Address*. Berikut adalah flowchart proses konfigurasi IP *Address* dan perancangan *hotspot* pada Mikrotik *RouterOS 5.18* pada gambar 3.4 konfigurasi IP *Address* dan gambar 3.5 perancangan *hotspot :*




Gambar 3.4 Konfigurasi IP *Address*

Pada proses konfigurasi IP *Address* ini, yang dimasukkan kedalam *address* yaitu IP *Address* yang dimiliki oleh Mikrotik *RouterOS 5.18*.Selain itu harus ditentukan juga *interface*nya. Jika langkah konfigurasinya berhasil dilakukan maka akan tampil hasil dari konfigurasi IP *Address.* Konfigurasi IP *address* diperlukan agar nanti saat proses perancangan *hotspot* berjalan dengan baik.




Gambar 3.5 Perancangan *Hotspot* pada Mikrotik RouterOS 5.18

*Hotspot* yang sudah terbangun akan mempermudah dalam penelitian ini, yaitu digunakan untuk proses *login* pada jaringan lokal. Jika proses yang dilakukan saat perancangan *hotspot* berhasil maka akan ditampilkan hasil perancangannya.

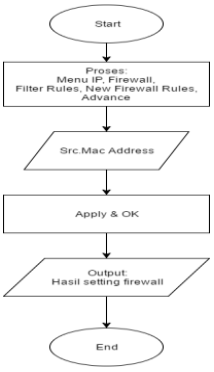
### 3.5.2 Perancangan Sistem Keamanan untuk Penanganan *MAC Clone* menggunakan Metode Proteksi *Firewall*

Sebelumnya pada sistem jaringan yang ada di STMIK Pradnya Paramita masih belum menggunakan keamanan internet yang mamadai, sehingga banyak pengguna lain yang tidak memiliki *user* bisa menggunakan internet yang ada di STMIK Pradnya Paramita dengan cara menduplikasi MAC *Address*. Pada penelitian ini peneliti mengembangkan yang sebelumnya sudah

ada keamanan internet yang belum memadai, menjadi ada keamanan internet yang cukup memadai dengan menggunakan metode proteksi dengan *firewall.*

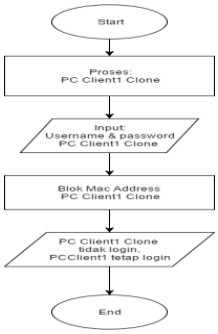
Metode proteksi *firewall* ini adalah sebuah cara untuk mengamankan keamanan internet yang ada di STMIK Pradnya Paramita yang awalnya pengguna bisa langsung menggunakan internet, dengan metode proteksi yang diterapkan ini pengguna harus terlebih dahulu meminta dibuatkan *username* dan *password* kepada admin untuk mengakses internet yang ada di STMIK Pradnya Paramita.

Berikut adalah proses keamanan internet menggunakan proteksi *firewall* seperti yang terlihat pada gambar 3.6 memblok MAC *Address :*




Gambar 3.6 Blok *MAC Address*

Berikut adalah hasil dari dilakukannya penambahan proteksi pada *firewall* pada gambar 3.7 :



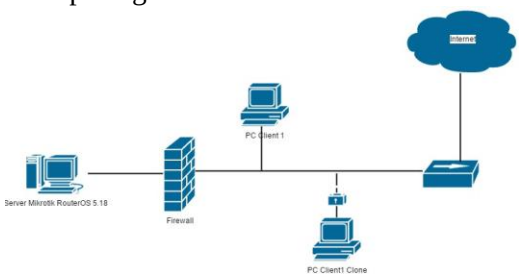

Gambar 3.7 Hasil *Login* Setelah dilakukan *setting* pada *firewall*

Pada awalnya sebelum ada setting pada *firewall* ketika ada *user* pada *client* yang secara illegal dapat dengan mudah mengambil alih hak autoritas *user* yang sudah memiliki *user* secara legal. Sehingga pemilik *user* yang asli akan secara otomatis *logout* ketika *user* yang sudah berhasil meng*cloning mac address* pemilik *user* yang asli.

Namun ketika sudah dibangun sistem keamanan dengan memanfaatkan *firewall* ini berjalan, sehingga ketika dilakukan *login* dengan MAC *address* yang sama secara otomatis tidak akan bisa dengan mudah *login* ke jaringan dan hak *autoritas* pemilik *user* asli dapat dikembalikan. Oleh karena itu, agar dapat *login* MAC *address* harus berbeda dan otomatis *username* dan *password* juga harus berbeda dan harus mendaftar dahulu kepada *administrator* jaringan.

### 3.5.3 Detail Alur Penyelesaian Masalah Penanganan *MAC Clone*

Setelah langkah – langkah pembuatan *flowchart diagram* keamanan jaringan *hotspot* mikrotik, berikut ilustrasi detail alur penyelesaian masalah penanganan *MAC Clone* pada gambar 3.8 :




Gambar 3.8 Detail Alur Penyelesaian Masalah

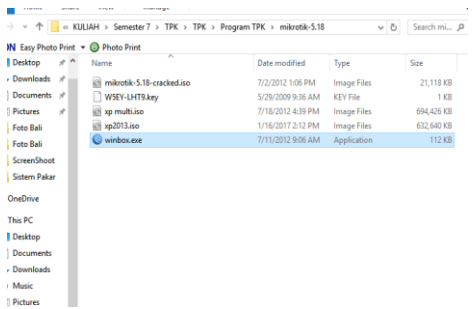
Setelah diterapkan dengan melakukan settingan pada *firewall*, informasi serta lalu lintas jaringan yang ada akan di*filter* (disaring). Sehingga *user* yang memiliki hak akses secara legal akan dapat mengakses jaringan lokal yang tersedia. Jika ada *user* yang tidak bertanggung jawab akan mengakses internet maka akan secara langsung di*lock* (dikunci) dan tidak dapat mengakses jaringan lokal.

## 4. HASIL PENELITIAN

### 4.1 Konfigurasi Penanganan *Mac Clone* dengan Menggunakan *Firewall*

#### 4.1.1 *Cloning PC Client1* yang Sudah Terinstall

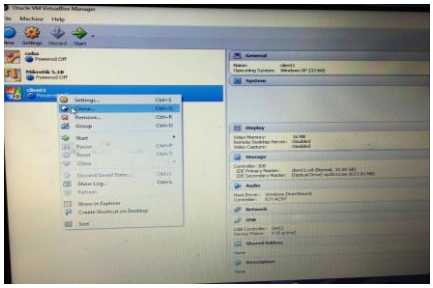
Siapkan beberapa file yang dapat dilihat seperti pada gambar 4.1.




Gambar 4.1 *File-file* yang dibutuhkan

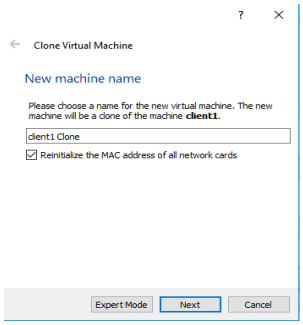
Untuk melakukan proses *cloning* PC *Client1*, pertama kita harus menyiapkan hasil installasi PC *Client1* pada *Virtualbox*. *VirtualBox* ini digunakan untuk membuat mikrotik serta PC secara *virtual*.

Selanjutnya untuk melakukaan *cloning* PC *Client1* dapat dilihat seperti pada gambar 4.2.



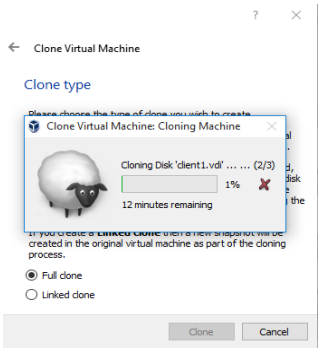
Gambar 4.2 *Cloning* PC *Client1*

Setelah pilih *clone* akan tampil perintah seperti yang ditunjukkan pada gambar 4.3.




Gambar 4.3 *Cloning* PC *Client1*

Ketika kita klik *button next* maka proses *cloning* PC sudah dimulai, untuk tampilan prosenya dapat dilihat pada gambar 4.4.



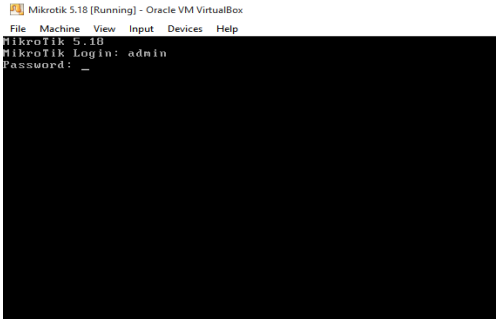

Gambar 4.4 *Cloning* PC *Client1*

Setelah selesai proses *cloning* PC , maka tampilannya tidak jauh berbeda dengan PC asli juga memiliki IP *Address* dan MAC *Address* yang sama. Tampilan PC *clone* pada gambar 4.5.


Gambar 4.5 Hasil *Cloning* PC *Client 1*

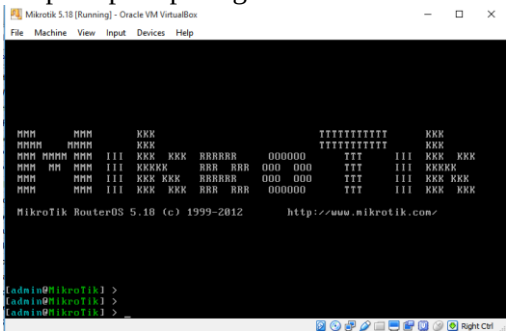
### 4.1.1.2 Konfigurasi *Interface* Jaringan

Sebelum melakukan konfigurasi *interface* aktifkan terlebih dahulu hasil dari virtual mikrotik *RouterOS 5.18* dengan cara *login* pada mikrotik terlebih dahulu, berikut tampilan dari mikrotik virtual yang sudah dibuat pada gambar 4.6.




Gambar 4.6 Mikrotik *Router*OS 5.18

Untuk *user login*nya menggunakan admin dan passwordnya kosong, enter kemudian sudah berhasil *login* ke mikrotik akan tampil seperti pada gambar 4.7.

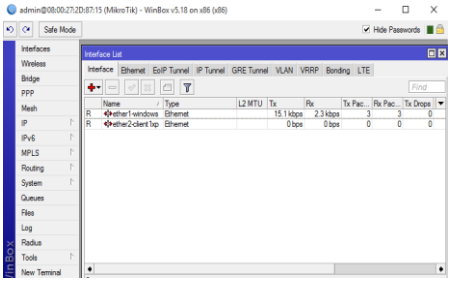



Gambar 4.7 Tampilan Mikrotik *Router*OS 5.18

Setelah mikrotik berhasil diaktifkan langkah selanjutnya adalah menyambungkannya pada *winbox*, untuk prosesnya pada gambar 4.8.


Gambar 4.8 *Login Winbox*

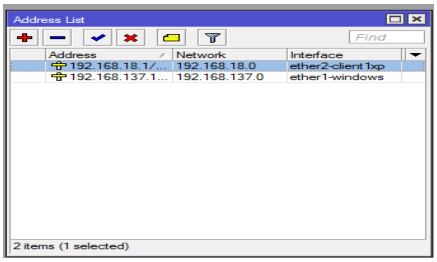
Untuk menyambungkan mikrotik ke *winbox* gunakan MAC *Address*nya mikrotik saja, agar tidak mudah keluar dari sistem *winbox* . Setelah berhasil maka akan masuk ke *server* mikrotik seperti yang ditunjukkan pada gambar 4.9.



Gambar 4.9 *Interface List*

### 4.1.1.3 Konfigurasi IP *Address*

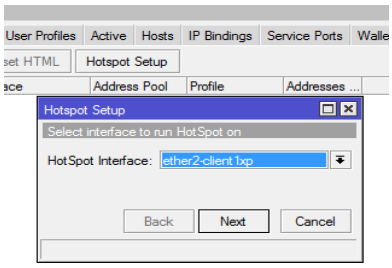
Konfigurasi pertama yang dilakukan yaitu dengan menambahkan IP *Address* pada *ether1* dan *ether2*. Untuk *ether1* menggunakan IP 192.168.137.1/24 dengan *network* 192.168.137.0 dan untuk *ether2* menggunakan IP 192.168.18.1/24 dengan *network* 192.168.18.0. Untuk proses konfigurasi IP *address* yaitu klik menu IP dan pilih *Addresses*. Setelah masuk *Address List* maka tambahkan IP untuk *interface ether1-windows* dan *ether2-client1xp* seperti pada gambar 4.10.




Gambar 4.10 Konfigurasi IP *Address*

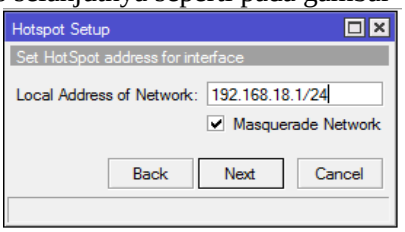
### 4.1.1.4 Konfigurasi *Hotspot*

Pada konfigurasi ini akan dilakukan proses pembangunan *hotspot* juga *setting hotspot*. Untuk proses konfigurasi *hotspot* yaitu klik menu IP, pilih *hotspot* konfigurasi *hotspot* dan klik tombol *button Hotspot Setup*. Untuk proses selanjutnya dimulai dari proses seperti pada gambar 4.11.



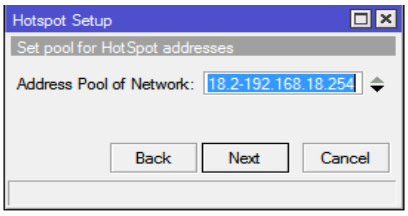

Gambar 4.11 *Hotspot Interface*

Untuk *hotspot interface* pilih *ether2-client1xp*, klik *next* kemudian lanjutkan proses selanjutnya seperti pada gambar 4.12.



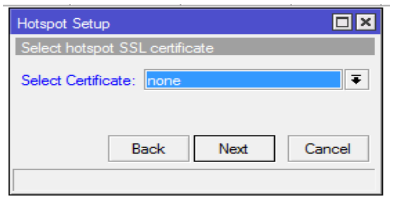

Gambar 4.12 *Local Address of Network*

Pada Lokal *address network* ini sudah secara otomatis muncul, klik *next* saja dan berlanjut pada tahap berikutnya pada gambar 4.13.



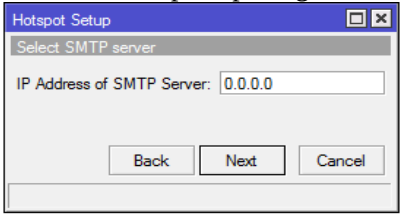

Gambar 4.13 *Address Pool of Network*

Tentukan rentang *address pool* yang dibutuhkan, isi dari *address pool* yaitu IP *address host* yang nantinya dapat terpasang pada PC ketika menggunakan jaringan *hotspot*. Tahap selanjutnya lihat pada gambar 4.14.




Gambar 4.14 *Select Certificate*

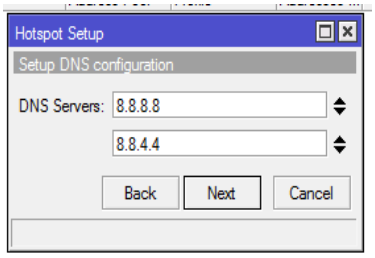
Tetapkan *none* saja, klik *next* berlanjut pada tahap selanjutnya menentukan IP *address* SMTP seperti pada gambar 4.15.




Gambar 4.15 IP *Address of* SMTP *Server*

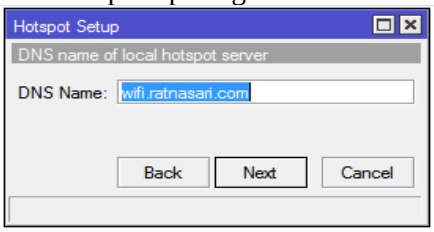
Tidak perlu diubah biarkan *default*nya saja 0.0.0.0, klik *next* beranjut

pada pengisian DNS *Server* seperti pada gambar 4.16.



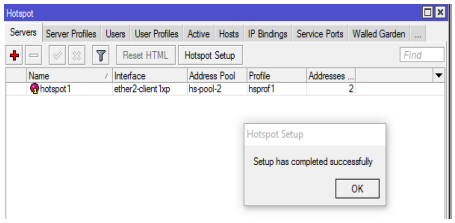

Gambar 4.16 DNS *Server*

Untuk DNS *Server* isikan 8.8.8.8 dan 8.8.4.4, klik *next* ke tahap pemberian DNS *name* seperti pada gambar 4.17



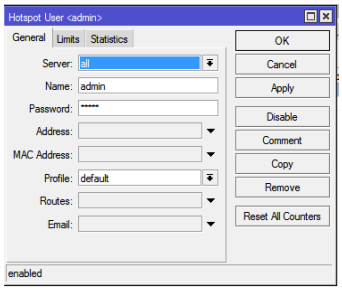

Gambar 4.17 DNS *Name*

DNS *name* kali ini dituliskan **wifi.ratnasari.com,** klik *next* maka akan tampil hasil konfigurasi *hotspot* seperti pada gambar 4.18.

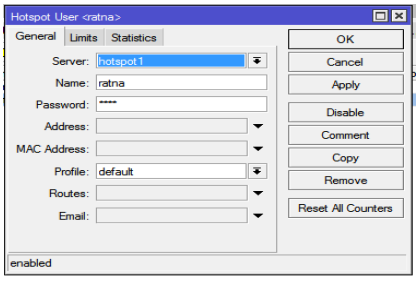



Gambar 4.18 Hasil Konfigurasi *Hotspot*

Pembuatan *username* dan *password* untuk *login* ke *hotspot*, seperti pada gambar 4.19 dan 4.20.

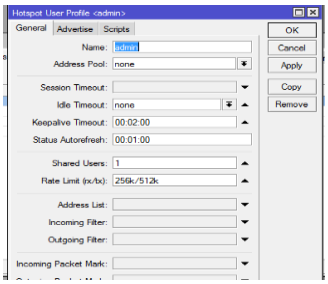



Gambar 4.19 *User* Admin

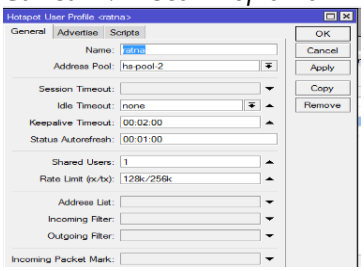



Gambar 4.20 *User* Ratna

Setelah membuat *username* dan *password*, selanjutnya membuat *User Profile*nya,*rate limit* untuk admin kali ini dibuat lebih tinggi daripada *rate limit* untuk ratna prosesnya seperti pada gambar 4.21 dan 4.22.

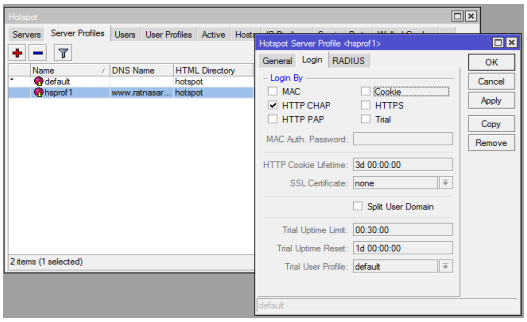



Gambar 4.21 *User Profile* Admin



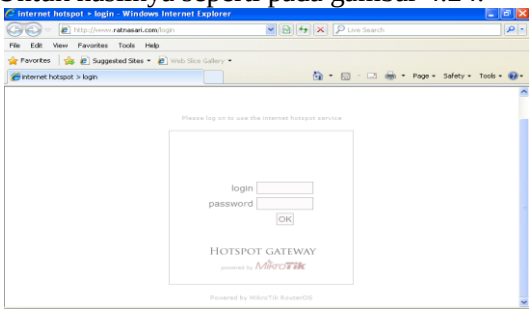

Gambar 4.22 *User Profile* Ratna

Untuk selanjutnya cara menonaktifkan *Cookies* pada DNS *name* **wifi.ratnasari.com**, bisa dilihat pada gambar 4.23.



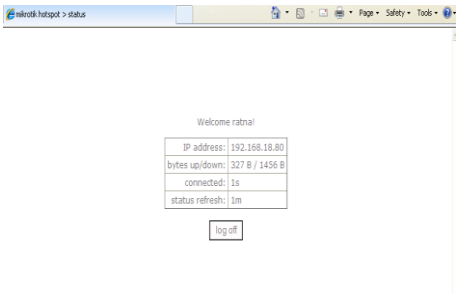

Gambar 4.23 Nonaktif *Cookies*

Sekarang lakukan tes *hotspot* yang sudah terbangun pada PC *Client1 virtual.* Untuk hasilnya seperti pada gambar 4.24.



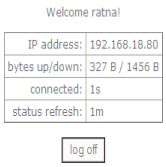

Gambar 4.24 Tes Hasil Konfigurasi *Hotspot*

Coba *login* pada PC *Client1* dengan menggunakan *user* yang sudah dibuat tadi, disini yang digunakan yaitu *user* ratna , untuk hasilnya dapat dilihat pada gambar 4.25.




Gambar 4.25 PC *Client1* Berhasil *Login*

Lakukan *login* juga pada PC *Client1 Clone* dengan menggunakan *username* dan *password* yang sama dengan PC Client1, hasilnya dapat dilihat pada gambar 4.26.

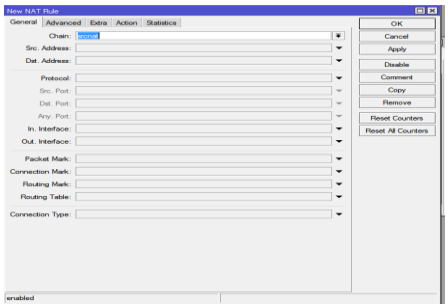



Gambar 4.26 PC *Client1 Clone Login*

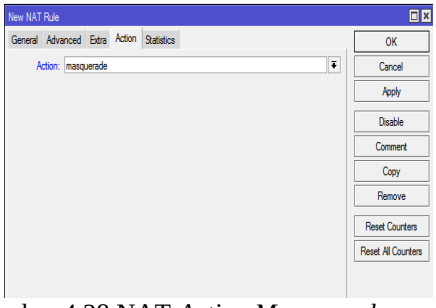
PC *Client1 Clone* juga berhasil masuk, tapi setelah kita cek PC *Client1* yang sudah *login* akan *logout* secara otomatis.

### 4.1.1.5 Konfigurasi *Firewall*

Pada tahap ini dilakukan konfigurasi *firewall* yaitu dilakukan *setting* pada NAT dan *Filter Rule.* Untuk proses konfigurasinya klik menu IP, pilih *firewall*, pilih NAT pada NAT ini dilakukan konfigurasi dengan menngunakan *chain srcnat* dan *Action*nya pilih masquerade, kemudian klik *apply* dan *ok.*Untuk prosesnya bisa dilihat pada gambar 4.27 dan 4.28.



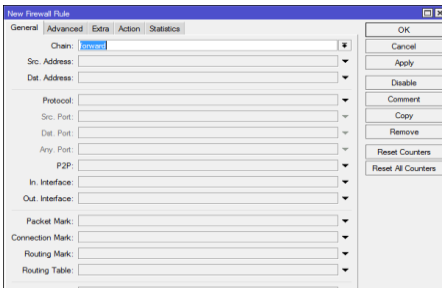

Gambar 4.27 NAT *Chain*




Gambar 4.28 NAT *Action Masquerade*

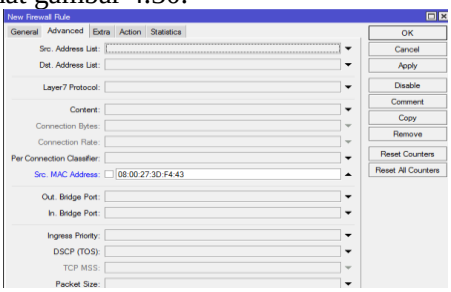
Klik *apply* dan *ok*, setelah melakukan *settingan* pada NAT, selanjutnya melanjutkan *settingan* pada *Firewall Rules.* Prosesnya yaitu klik *button firewall rule* maka akan tampil menu – menunya. Untuk prosesnya bisa dilihat pada gambar 4.29, gambar 4.30, dan gambar 4.31.

Chain isikan *forward*, lihat gambar 4.29.



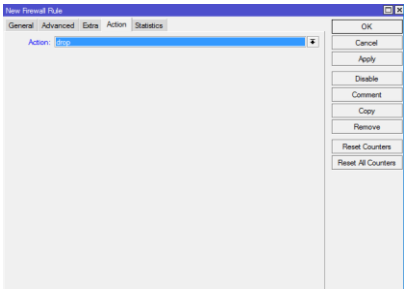

Gambar 4.29 *Chain Firewall Rule*

Isikan MAC *address* yang akan di blok, lihat gambar 4.30.



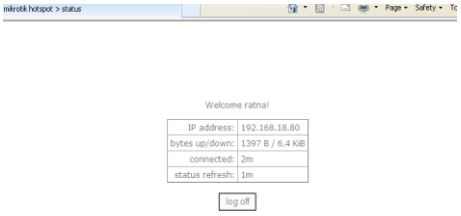

Gambar 4.30 *Src.MAC Address*

Untuk *actionnya* pilih *drop, lihat gambar 4.31.*



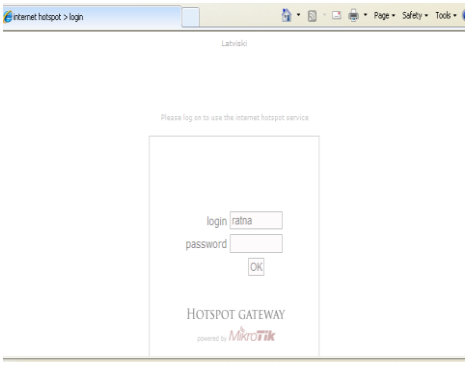

Gambar 4.31 *Firewall Rule Action*

Setelah semua *settingan firewall* selesai selanjutnya dilakukan tes jaringan *hotspot.* Pertama *login* PC *Client1* terlebih dahulu. Untuk hasilnya bisa dilihat pada gambar 4.32.



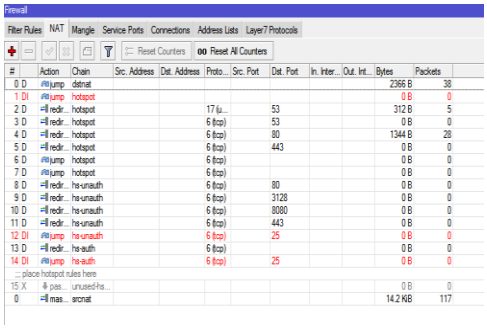

Gambar 4.32 *Login* PC *Client1*

Selanjutnya *login* PC *Client1 Clone* dengan menggunakan *username* yang sama. Untuk hasilnya bisa dilihat pada gambar 4.33.

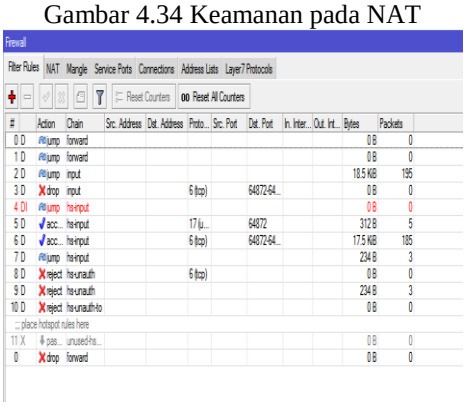



Gambar 4.33 PC *Client1 Clone* Gagal Login

Meskipun sudah gagal *login*, PC *Client Clone* tetap akan terdeteksi, karena sudah mengakses DNS *name* **wifi.ratnasari.com.**




Gambar 4.34 Keamanan pada NAT




Gambar 4.35 Keamanan Pada *Filter Rule*

## 5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, maka dapat diambil beberapa kesimpulan:

1. Dengan terbangunnya keamanan internet menggunakan *firewall* yaitu melakukan *setting* pada *filter rules* dan NAT membantu pengguna untuk meminimalisir terjadinya *MAC-Cloning.*
2. Dengan dilakukannya pemblokan pada *MAC-Address Cloning, user* illegal tidak dapat dengan mudah untuk mengambil alih hak akses pemilik *user* asli.
3. Dengan dilakukannya monitoring melalui *hotspot* dapat diketahui siapa saja yang masuk ke dalam jaringan yang sudah terbangun.

## 6. REFERENSI


Abdullah, Imam Marzuki, Misdiyanto. *Optimalisasi Bandwidth Dengan Filterisasi Menggunakan Mikrotik Routerboard di Universitas Panca Marga Probolinggo*. Vol. 4 No. 2 Nopember 2014 36-47. ISSN: 2088-4591.

Anjik Sukmaji, dan Rianto. 2008. *Jaringan Komputer Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan***.** Yogyakarta: Andi.

Arifin Zainal, *E-Bussines membangun bisnis hosting dan domain*. Jakarta: PT.Elex Media Komputindo.

Davidson Jonatan, Tina Fox.2002,*Developing Cisco Voie Over Ip Solution***.** ***Cisco press: Indianapolis USA***.

Enterprise Jubilee,2009.*100 Tip & Trik Wi-Fi*. Jakarta: PT.Elex Media Komputindo.

Fatsyahrina Fitriastuti, Dodi Prasetyo Utomo. 2014. *Implementasi Bandwith Management dan Firewall System Menggunakan Mikrotik OS 2.9.27*. Vol. 4, No. 1, April 2014 1-9. ISSN: 2088 – 3676.

Kustanto, dan Saputro, Daniel. 2008. *Membangun Server Internet Dengan Mikrotik OS.* Yogyakarta: Gava Media.

Muryanto ,Prasetyo Uji. Implementasi Sistem *Wireless Security* dan *Managemen Bandwidth* Berbasis *Radius Server Dengan Mikrotik Di LEMHANNAS Republlik Indonesia.*

Purwanto Eko. 2015. Implementasi Jaringan *Hotspot* dengan Menggunakan *Router Mikrotik sebagai Penunjang Pembelajaran (Studi Kasus:SMK Sultan Agung Tirtomoyo Wonogiri).* Vol. 1 No. 2 Tahun 2015 20-27. ISSN : 2442-7942.

Prasad. 2005. *Implementasi Jaringan Wireless*. Yogyakarta: Andi Offset.

Siswo Wardoyo, Taufik Ryadi, Rian Fahrizal. *Analisis Performa File Transport Protocol Pada Perbandingan Metode IPv4 Murni, IPv6 Murni dan Tunneling 6to4 Berbasis Router Mikrotik.* Vol. 3 No. 2

September 2014 106-117. ISSN: 2302 – 2949.

Solehudin Arip.2015. *Implementasi Arsitektur Jaringan dan Penerapan Limiting Upload/Download File Extensions Menggunakan Mikrotik Router di Laboratorium Komputer UNSIKA.* Vol. 2 No. 6 Juni 2015 – Agustus 2015 1-10. ISSN:2355-1119.

Wahana Komputer. 2014. *Mikrotik Menggunakan Metode Virtualisasi.* Yogyakarta: Andi.