SKRIPSI

ANALISIS DAN IMPLEMENTASI FIREWALL DENGAN METODE PORT ADDRESS TRANSLATION PADA MIKROTIK OS

Oleh:

FITRI RAMADHANI H.
NIM: K105 82 1675 15

ABDUL MUZAKKIR YAHYA MT.
NIM: K105 82 1709 15

FAKULTAS TEKNIK

PROGRAM STUDI TEKNIK ELEKTRO

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2018

ANALISIS DAN IMPLEMENTASI *FIREWALL* DENGAN METODE *PORT ADDRESS TRANSLATION* PADA MIKROTIK ROUTER OS

Skripsi

Diajukan sebagai salah satu syarat

untuk memperoleh gelar Sarjana

Program Studi Teknik Telekomunikasi

Jurusan Teknik Elektro

Fakultas Teknik

Disusun Dan diajukan oleh :

FITRI RAMADHANI H.
NIM: K105 82 1675 15

ABDUL MUZAKKIR YAHYA MT.
NIM: K105 82 1709 15

PADA

UNIVERSITAS MUHAMMADIYAH MAKASSAR

MAKASSAR

2018

UNIVERSITAS MUHAMMADIYAH MAKASSAR
FAKULTAS TEKNIK
GEDUNG MENARA IQRA LT. 3
Jl. Sultan Alauddin No. 259 Telp. (0411) 866 972 Fax (0411) 865 588 Makassar 90221
Website: www.unismuh.ac.id, e_mail: unismuh@gmail.com
Website: http://teknik.unismuh.makassar.ac.id

بسم الله الرحمن الرحيم

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan untuk memenuhi syarat ujian guna memperoleh gelar Sarjana Teknik (ST) Program Studi Teknik Listrik Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Makassar.

Judul Skripsi : **Analisis Dan Implementasi Firewall Dengan Metode Port Address Transaltion Pada Mikrotik OS**

Nama : Fitri Ramadhani
Abdul Muzakkir Yahyah Maulana Tadjuddin

Stambuk : K105 82 1675 15
K105 82 1709 15

Makassar, 13 Februari 2018

Telah Diperiksa dan Disetujui
Oleh Dosen Pembimbing;

Pembimbing I	Pembimbing II
Dr. Ir. Hafsah Nirwana, M.T	**Rizal Ahdiyat Duyo, S.T.,M.T**

Mengetahui,
Ketua Jurusan Elektro

Dr. Umar Katu, S.T., M.T.
NBM : 990 410

UNIVERSITAS MUHAMMADIYAH MAKASSAR
FAKULTAS TEKNIK
GEDUNG MENARA IQRA LT. 3
Jl. Sultan Alauddin No. 259 Telp. (0411) 866 972 Fax (0411) 865 588 Makassar 90221
Website: www.unismuh.ac.id, e_mail: unismuh@gmail.com
Website: http://teknik.unismuh.makassar.ac.id

بسم الله الرحمن الرحيم

PENGESAHAN

Skripsi atas nama Fitri Ramadhani H.dengan nomor induk Mahasiswa K10582 1675 15 dan Abdul Muzakkir Yahyah Maulana Tadjuddin dengan nomor induk Mahasiswa K10582 1709 15 dinyatakan diterima dan disahkan oleh Panitia Ujian Tugas Akhir/Skripsi sesuai dengan Surat Keputusan Dekan Fakultas Teknik Universitas Muhammadiyah Makassar Nomor : 0002/SK-Y/20201/091004/2018, sebagai salah satu syarat guna memperoleh gelar Sarjana Teknik pada Program Studi Teknik Listrik Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Makassar pada hari Senin tanggal 12 Februari 2018.

Makassar, 27 Jumadil Awal 1439 H / 13 Februari 2018 M

Panitia Ujian :

1. Pengawas Umum
   a. Rektor Universitas Muhammadiyah Makassar
      Dr. H. Abdul Rahman Rahim, SE., MM. : .....
   b. Dekan Fakultas Teknik Universitas Hasanuddin
      Dr. –Ing. Ir. Wahyu H. Piarah,MSME. : .....
2. Penguji
   a. Ketua : Dr.Ir.Zulfajri Basri Hasanuddin,M.Sc.M.Eng: .....
   b. Sekertaris : Andi Abd Halik Lateko, ST.,MT : .....
3. Anggota : 1. Dr. Ir. Zahir Zainuddin, M.Sc : .....
   2. Rahmania,ST.,MT : .....
   3. Rossy Timur Wahyuningsih,ST.,MT : .....

Mengetahui :

Pembimbing I	Pembimbing II
Dr. Ir. Hafsah Nirwana, M.T	**Rizal Ahdiyat Duyo, S.T.,M.T**

Dekan

Ir. Hamzah Al Imran, S.T., M.T.
NBM : 855 500

KATA PENGANTAR

Syukur Alhamdulillah penulis panjatkan kehadirat Allah SWT, karena rahmat dan hidayah-Nyalah sehingga penulis dapat menyusun skripsi ini, dan dapat kami selesaikan dengan baik.

Tugas akhir ini disusun sebagai salah satu persyaratan Akademik yang harus ditempuh dalam rangka menyelesaikan Program Studi pada Jurusan Teknik Telekomunikasi Fakultas Teknik Universitas Muhammadiyah Makassar. Adapun Judul tugas akhir kami adalah : ”Analisis dan Implementasi Firewall dengan Metode Port Address Translation Pada Mikrotik Router OS”.

Penulis menyadari sepenuhnya bahwa di dalam penulisan skripsi ini masih terdapat kekurangan-kekurangan, hal ini disebabkan penulis sebagai manusia biasa tidak lepas dari kesalahan dan kekurangan baik itu ditinjau dari segi teknis penulisan maupun dari perhitungan-perhitungan. Oleh karena itu, penulis menerima dengan ikhlas dan senang hati segala koreksi serta perbaikan guna penyempurnaan tulisan ini agar kelak dapat bermanfaat.

Skripsi ini dapat terwujud berkat adanya bantuan, arahan, dan bimbingan dari berbagai pihak. Oleh karena itu dengan segala ketulusan dan kerendahan hati, kami mengucapkan terima kasih dan penghargaan yang setinggi-tingginya kepada

1. Bapak Ir. Hamzah Al Imran, S.T., M.T. sebagai Dekan Fakultas Teknik Universitas Muhammadiyah Makassar.
2. Bapak Umar Katu, S.T.,M.T. sebagai Ketua Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Makassar.

3. Ibu Dr. Ir. Hafsah Nirwana, M.T. selaku Pembimbing I dan Bapak Rizal A. Duyo S.T., M.T. selaku Pembimbing II yang telah banyak meluangkan waktu dalam membimbing kami.
4. Bapak dan Ibu dosen serta staf pegawai pada Fakultas Teknik atas segala waktunya telah mendidik dan melayani penulis selama mengikuti proses belajar mengajar di Universitas Muhammadiyah Makassar.
5. Seluruh staf pengajar pada program studi Teknik Elektro yang telah memberikan banyak arahan dan bimbingan.
6. Ayahanda dan Ibunda tercinta, penulis mengucapkan terima kasih yang sebesar-besarnya atas segala limpahan kasih sayang, doa dan pengorbanannya terutama dalam bentuk materi dalam menyelesaikan kuliah.
7. Rekan-rekan mahasiswa Teknik Elektro, khususnya kelas konversi program studi Teknik Telekomunikasi angkatan 2015 yang telah memberikan bantuan dan dukungannya selama penulis membuat proyek akhir ini.

Semoga semua pihak tersebut di atas mendapat pahala yang berlipat ganda di sisi Allah SWT dan skripsi yang sederhana ini dapat bermanfaat bagi penulis, rekan-rekan, masyarakat serta bangsa dan negara. Amin.

Makassar, 2018

Penulis

Fitri Ramadhani H[1], Muzakkir Yahya[2]
[1]Jurusan Teknik Elektro Fakultas Teknik Unismuh Makassar
email:fitri.ramadhani2550@gmail.com
[2]Jurusan Teknik Elektro Fakultas Teknik Unismuh Makassar
email: muzakkir.yahya57@gmail.com

ABSTRAK

Kebutuhan sistem keamanan jaringan komputer baik untuk sistem informasi atau komputer yang terhubung dengan jaringan internet, sangat rentan sekali terhadap penyusupan, pencurian data serta penyalahgunaan informasi oleh orang yang tidak bertanggung jawab. Sehingga upaya untuk melindungi sistem tersebut sangat dibutuhkan. *Firewall* merupakan salah satu solusi perlindungan jaringan komputer dalam mencegah adanya tindakan tersebut. metode yang diterapkanpun bermacam-macam meliputi *Circuit Level gateway*, *Application level gateway*, dan *Packet Filtering* firewall. Sebagai contoh adalah metode *Packet Filtering*, lalu lintas data akan di *filter* pada *layer network* meliputi *IP Address* dan *Port*, akan tetapi semakin meningkatknya kebutuhan keamanan, maka dibutuhan suatu keamanan yang dapat menginspeksi lebih dari satu lapisan *protokol* jaringan didalam satu sistem, sedangkan untuk menerapkan keamanan tersebut dibutuhkan suatu infrastruktur dan perangkat yang tidak murah. Sehingga diperlukan suatu perangkat dan sistem keamanan *firewall* yang ekonomis,efisien sekaligus mampu bekerja secara optimal untuk melindungi jaringan komputer. metode PAT (*Port Address Translation*) adalah suatu perancangan keamanan jaringan server yang memanfaatkan fungsi PAT pada perangkat *firewall*. *Mikrotik* merupakan salah satu *Operating System* yang mempunyai fitur unggulan, salah satunya adalah sebagai *Firewall*. Laporan tugas akhir ini akan menguraikan aktifitas dan produk yang dihasilkan pada masing-masing tahap pengembangan. Analisis dan implementasi *firewall multilayer* ini akan menghasilkan sebuah metode keamanan berlapis dengan meningkatkan pemfilteran yang lebih selektif, kemudahan administrasi sistem dan pengelolaanya. Pada tahap akhir pengembangan metode *firewall*, hal-hal apa yang telah dilakukan dan apa yang belum dilakukan pada pengembangan *firewall* ini akan diulas dan di evaluasi pada bagian akhir laporan ini.

Kata Kunci : *firewall, Packet Filtering, port address translation, mikrotik*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

A. Latar Belakang

Firewall merupakan salah satu solusi perlindungan jaringan komputer dalam mencegah serangan dan penyusupan yang dapat membahayakan kerahasiaan data serta kerusakan pada infrastruktur suatu jaringan. Mekanisme yang diterapkan baik terhadap *hardware, software* ataupun sistem itu sendiri dengan tujuan melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah *workstation, server, router,* atau *local area network* (LAN). Pada masing-masing jenis firewall tersebut, masih terdapat suatu kekurangan yaitu software *firewall* yang memakan sumber daya dari komputer (CPU, *memory*, *ruang disk*) sehingga dapat menyebabkan inkompatibilitas pada sistem operasi, sedangkan *hardware firewall* cenderung lebih mahal dan konfigurasi yang sangat sulit dibandingkan dengan *software firewall*, dengan demikian dibutuhkan suatu sistem *firewall* yang mampu berjalan dalam satu sistem yang efisien.

Beberapa metode *firewall* diantaranya adalah *Packet Filtering firewall* dan *Network Address Translation* (NAT). Untuk memenuhi kebutuhan keamanan pada segmen jaringan komputer secara efektif dan aman dibutuhkan suatu *firewall*

yang dapat menerapkan keamanan berlapis yang dapat menginspeksi di banyak layer protokol jaringan.

Selain dua metode diatas juga dapat diterapkan metode *Port Address Translation* yang merupakan suatu perancangan keamanan jaringan *server* yang memanfaatkan fungsi PAT pada perangkat *firewall.* PAT sendiri adalah salah satu fitur dari NAT (*Network Address Translation*) yang menerjemahkan protocol TCP atau UDP yang dibuat antara host atau *client* di jaringan lokal dengan *host* atau *server* pada jaringan *public* atau *local* lainnya. *Mikrotik* merupakan salah satu *Router Operating System* yang mempunyai banyak fitur, salah satunya adalah sebagai *Router* dan *Firewall.* Dalam penelitian ini penulis menganalisa kelemahan dan kekurangan pada metode *firewall* sebelumnya yaitu metode *packet filtering* dan menerapkan metode baru dengan mengkobinasikan metode *Port Address Translation* pada Mikrotik Router OS.

Berdasarkan latar belakang permasalahan tersebut maka penulis memilih judul: "Analisis dan Implementasi Firewall dengan metode Port Address Translation pada Mikrotik Router OS". Adanya penelitian ini agar didapatkan suatu analisa firewall yang aman dengan tingkat keamanan tinggi serta menghasilkan penerapan metode Port Address Translation pada Mikrotik Router OS.

B. Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan diatas maka rumusan masalahnya sebagai berikut:

1. Bagaimana menganalisa metode keamanan jaringan komputer dalam penerapan Firewall menggunakan metode port address translation (PAT) pada Mikrotik Router OS.
2. Bagaimana menganalisa metode keamanan jaringan komputer dalam penerapan Firewall menggunakan metode Packet Filter (access list).
3. Bagaimana menganalisis perbandingan metode Port Address Translation dengan metode Packet Filter (access list) sehingga didapatkan analisa dan metode terbaik.

C. Tujuan Penelitian

Berdasarkan rumusan masalah diatas maka tujuan yang dapat dicapai adalah:

1. Dapat menganalisa metode keamanan jaringan komputer dalam penerapan Firewall menggunakan metode Port Address Translation (PAT) pada Mikrotik Router OS.
2. Dapat menganalisa metode keamanan jaringan komputer dalam penerapan Firewall menggunakan metode Packet Filter (access list).
3. Dapat menganalisis perbandingan metode Port Address Translation dengan metode Packet Filter (access list) sehingga didapatkan analisa dan metode terbaik.

D. Batasan Masalah

Untuk menghindari pembahasan yang melebar, penulis melakukan analisis perbandingan terhadap metode Port Address Translation dengan metode Packet Filter pada Mikrotik Router OS.

E. Manfaat Penelitian

Manfaat dari penelitian ini yaitu menghasilkan keamanan pada jaringan pribadi dari hal yang membahayakan infrastruktur jaringan atau penyalahgunaan hak akses dari jaringan luar dengan memanfaatkan *Mikrotik Router OS* sebagai *firewall*.

F. Sistematika Penulisan

Bab I Menjelaskan tentang pendahuluan laporan yang meliputi latar belakang, rumusan masalah, tujuan, batasan masalah dan sistematika penulisan.

Bab II Menjelaskan tentang tinjauan pustaka yang mendukung pemahaman penulis untuk melaksanakan penelitian yang berkaitan dengan penerapan Firewall menggunakan metode port address translation (PAT) pada Mikrotik Router OS untuk meningkatkan keamanan pada satu system.

Bab III Menjelaskan tentang metodologi penelitian, tahapan penelitian (*flowchart*) Firewall menggunakan metode port address translation (PAT) pada Mikrotik Router OS.

Bab IV Menjelaskan tentang pengolahan data dan analisis system Firewall menggunakan metode port address translation (PAT) pada Mikrotik Router OS.

Bab V Menjelaskan tentang kesimpulan dan saran penulis.

BAB II

TINJAUAN PUSTAKA

A. Keamanan Jaringan Komputer

Tujuan utama dari keamanan sistem adalah memberikan jalur yang aman antar-entitas yang saling bertukar informasi dan untuk menyediakan perlindungan data. Insiden keamanan jaringan komputer adalah suatu aktivitas yang berkaitan dengan jaringan komputer, di mana aktifitas tersebut memberikan implikasi terhadap keamanan.

B. Jenis Serangan Terhadap Keamanan

Pada dasarnya, menurut jenisnya, serangan terhadap suatu data dalam suatu jaringan dapat dikategorikan menjadi 2, yaitu :

1. Serangan Pasif (Passive Attacks)

   Serangan pasif adalah serangan pada sistem autentikasi yang tidak menyisipkan data pada aliran data (data stream), tetapi hanya mengamati atau memonitor pengiriman informasi ke tujuan. Informasi ini dapat digunakan di lain waktu oleh pihak yang tidak bertanggung jawab. Serangan pasif yang mengambil suatu unit data dan kemudian menggunakanya untuk memasuki sesi autentikasi dengan berpura-pura menjadi user autentik/ asli disebut dengan replay attack. Beberapa informasi autentikasi seperti password atau data biometric yang dikirim melalui transmisi elektronik dapat direkam dan kemudian digunakan

untuk memalsukan data yang sebenarnya. Serangan pasif ini sulit untuk dideteksi karena penyerang tidak melakukan perubahan data. Oleh sebab itu untuk mengatasi serangan pasif ini lebih ditekankan pada pencegahan daripada pendeteksiannya.

2. Serangan Aktif (Active Attacks)

   Serangan aktif adalah serangan yang mencoba memodifikasi data, mencoba mendapatkan autentikasi, atau mendapatkan autentikasi dengan mengirimkan paket-paket data yang salah ke data stream atau dengan memodifikasi paket-paket yang melewati data stream. Kebalikan dari serangan pasif, serangan aktif sulit untuk dicegah karena untuk melakukannya dibutuhkan perlindungan fisik untuk semua fasilitas komunikasi dan jalur-jalurnya setiap saat. Yang dapat dilakukan adalah mendeteksi dan memulihkan keadaan yang disebabkan oleh serangan ini.

C. Model OSI

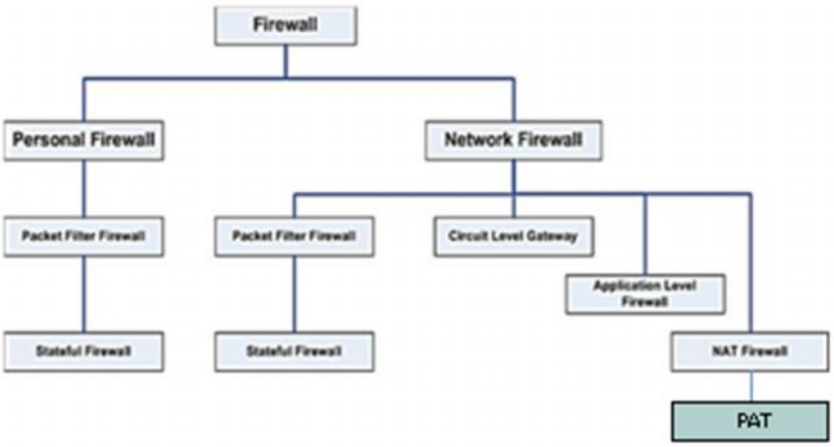
Model OSI ditetapkan oleh sebuah badan standar internasional yang bernama *International Standards Organization (ISO)* pada tahun 1947. Standar semacam ini perlu untuk menjaga interoperabilitias antar peralatan yang dibuat oleh pabrik yang berbeda-beda. Model OSI menetapkan 7 lapis proses, yaitu Application layer, Presentation layer, Session layer, Transport layer, Network layer, Data- link layer dan Physical layer.

D. Protokol

Protokol adalah sebuah standar aturan yang mengatur alat-alat dalam jaringan komputer sehingga dapat saling berkomunikasi satu sama lain, dapat berhubungan satu sama lain dan dapat melakukan perpindahan data satu sama lain. Protokol dapat diterapkan pada perangkat keras (hardware), perangkat lunak (software) dan kombinasi keduanya.

E. Definisi Firewall

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan lingkupnya. Segmen tersebut dapat merupakan *sebuah workstation, server, router,* atau *local area network* (LAN).



Gambar 2.1 Skema *Firewall* pada *Mikrotik OS*

1. Fungsi Firewall

Berdasarkan definisi diatas Fungsi umum firewall adalah :

a) Mengatur dan mengontrol lalu lintas jaringan

b) Melakukan autentikasi terhadap akses

c) Melindungi sumber daya dalam jaringan privat

d) Mencatat semua kejadian, dan melaporkan kepada administrator.

2. Karakteristik Firewall

Berikut ini adalah karakteristik dari sebuah *firewall* :

a) Seluruh hubungan/kegiatan dari dalam ke luar, harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud.

b) Hanya kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat di lakukan dengan mengatur *policy* pada konfigurasi keamanan lokal. Banyak sekali jenis *firewall* yang dapat di pilih sekaligus berbagai jenis *policy* yang di tawarkan.

c) *Firewall* itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. Hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem yang relatif aman.

F. NAT (Network Address Translation)

NAT (Network Address Translation) firewall secara otomatis menyediakan proteksi terhadap sistem yang berada di balik firewall karena NAT firewall hanya mengizinkan koneksi yang datang dari komputer-komputer yang berada di balik firewall. Tujuan dari NAT adalah untuk melakukan *multiplexing* terhadap lalu lintas dari jaringan internal untuk kemudian menyampaikannya kepada jaringan yang lebih luas (MAN, WAN atau Internet) seolah-olah paket tersebut datang dari sebuah alamat IP atau beberapa alamat IP. NAT Firewall membuat tabel dalam memori yang mengandung informasi mengenai koneksi yang dilihat oleh firewall. Tabel ini akan memetakan alamat jaringan internal ke alamat eksternal. Kemampuan untuk menaruh keseluruhan jaringan di belakang sebuah alamat IP didasarkan terhadap pemetaan terhadap port-port dalam NAT firewall.

Ada tiga tipe NAT yang dapat dipakai, yaitu :

1. Static NAT

Pada static NAT, setiap *IP address* pribadi ditranslasikan secara tetap dengan satu *IP* publik tertentu. Peralatan router memiliki dua sisi. Sisi luar (outside) memiliki IP address publik yang berhubungan dengan internet dan sisi dalam memliki IP address pribadi yang berhubungan dengan LAN. Prinsip kerja NAT sangat sederhana, secara manual anda membuat agar NAT mentrasnlasikan setiap IP address pribadi yang dimiliki oleh komputer dengan suatu IP address publik yang anda miliki.

2. Dynamic NAT

Pada Dynamic NAT, setiap *IP address* pribadi ditranslasikan secara dinamis dengan satu *IP address* publik yang tersedia. Adakalanya anda menginginkan agar satu kelompok IP address pribadi ditranslasikan ke satu kelompok IP address publik secara otomatis oleh NAT. apabila salah satu IP address pribadi dari kelompok akan di pakai, maka IP address pribadi tersebut akan ditranslasikan pada IP address publik pertama yang mana saja tersedia jadi translasi hanya terjadi jika sedang dipakai. Oleh sebab itu translasi berubah-ubah sesuai dengan kebutuhan. NAT tipe ini disebut dynamic karena berubah-ubah. Keuntungan tipe dynamic NAT ini adalah jumlah IP address publik yang diperlukan oleh lebih sedikit dari jumlah IP address pribadi yang anda miliki, karena pada umumnya tidak semua IP address pribadi akan dipakai pada saat yang bersamaan.

3. PAT (Port Address Translation)

Port Address Translation (PAT) adalah suatu fitur dari jaringan perangkat yang menerjemahkan TCP atau UDP, komunikasi yang dilakukan antara host pada jaringan pribadi dan host pada jaringan.

Perangkat PAT memodifikasi IP paket secara transparan seperti saat melewatinya. Modifikasi yang membuat semua paket yang mengirim ke jaringan publik dari beberapa host di jaringan pribadi tampaknya berasal dari satu host, (perangkat PAT) pada jaringan publik.adapun hubungan antara NAT dan PAT yaitu PAT adalah bagian dari NAT, dan terkait erat dengan konsep Network Address Translation . PAT juga dikenal sebagai NAT Overload. Dalam PAT pada

umumnya hanya satu alamat IP publik terbuka dan beberapa host privat menghubungkan melalui alamat yang tertera. Masuknya paket dari jaringan publik diarahkan pada jaringan privat dengan mengacu pada tabel dalam perangkat PAT yang melacak port pairs publik dan privat.

Dalam PAT, baik pengirim pribadi IP dan nomor port diubah, perangkat PAT memilih nomor port yang akan dilihat oleh host pada jaringan publik. Dalam hal ini, PAT beroperasi pada layer 3 (jaringan) dan 4 (transportasi) dari model OSI , sedangkan NAT dasar hanya beroperasi pada layer 3.

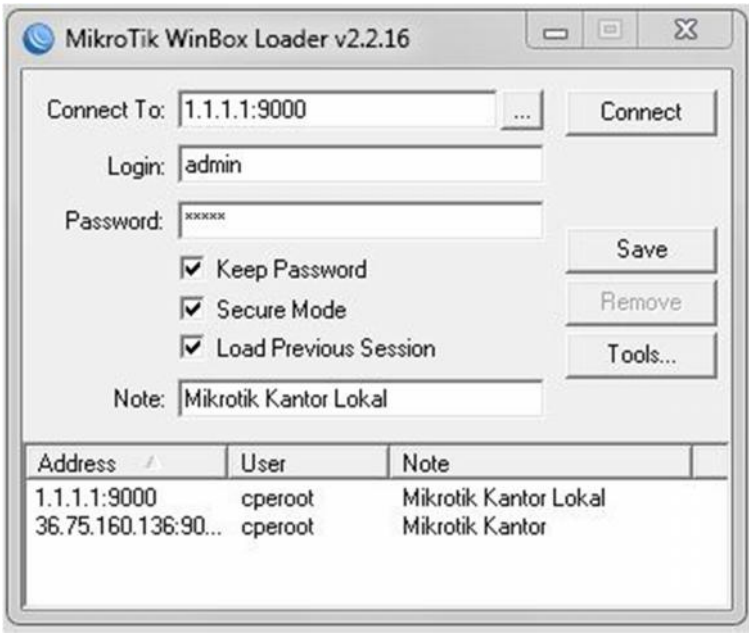
G. Gateway

Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan komputer dapat diberikan kepada jaringan komputer yang protokolnya berbeda.

Gambar 2.2 Gateway (Mikrotik rb951ui-2nd)

H. Winbox

Winbox adalah sebuah utility yang digunakan untuk melakukan remote ke server mikrotik dalam mode GUI (*Graphical User Interface).*



Gambar 2.3 Tampilan WinBox v2.2.16

I. TFGen

Aplikasi TFGen adalah salah satu aplikasi yang dapat digunakan untuk melakukan serangan ke salah satu host, server atau perangkat lainnya yang berbasis IP berupa traffic (UDP Protocol) dimana besaran traffic dapat diatur dan dikirim secara terus menerus.

BAB III

METODOLOGI PENELITIAN

G. Tempat dan Waktu Penelitian

Penelitian ini dilakukan pada tanggal 1 Oktober-26 November 2017 yang berlokasi di Makassar.

Tabel 3.1 Waktu Perencanaan Penelitian

NO	Kegiatan	Minggu Ke-			
		I	II	III	IV
1	Studi Literatur				
2	Pengumpulan Alat dan Bahan Penelitian				
3	Perancangan sistem jaringan meliputi Server dan Client				
4	Pembandingan hasil metode Port Address Translation dan metode Packet Filtering serta analisis Data				
5	Kesimpulan				

B. Objek Penelitian

Objek dari penelitian ini adalah implementasi metode Port Address Translation dan metode Packet Filtering pada Server.

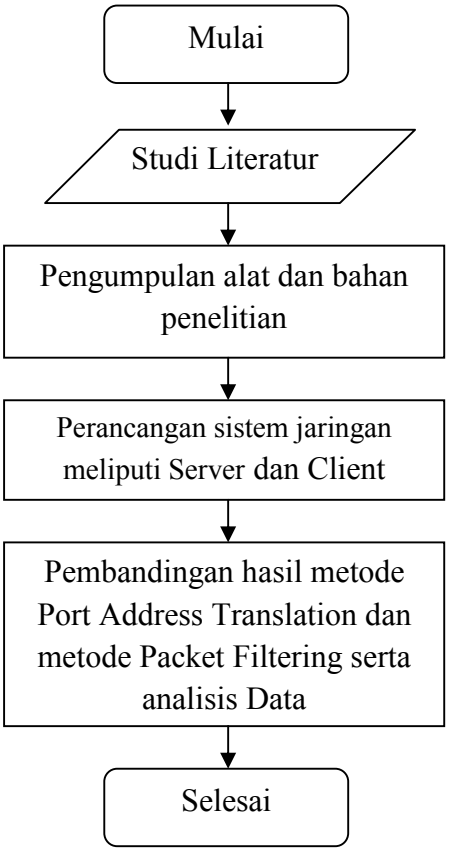
C. Alat dan Bahan

1. Laptop
2. Handphone
3. Mikrotik (*Gateway*)

4. Kabel UTP
5. Aplikasi WinBox v2.2.16 (*Gateway*)
6. Aplikasi TFGen

D. *Flowchart* Penelitian

Flowchart adalah suatu metode untuk menggambarkan tahap-tahap pemecahan masalah dengan mempresentasikan simbol – simbol tertentu yang mudah dimengerti. Tujuan utama dari penggunaan *flowchart* adalah untuk menggambarkan suatu tahapan penyelesaian masalah secara sederhana, terurai dan jelas menggunakan simbol – simbol yang standar.



Gambar 3.1 *Flowchart* Penelitian

E. Metodologi Penelitian

1. Studi Literatur

   Kegiatan studi pustaka dilakukan dengan mempersiapkan literatur pada berbagai sumber yang berhubungan dengan topik penelitian berupa dokumen, buku teks, jurnal, *web* hingga media elektronik seperti video.

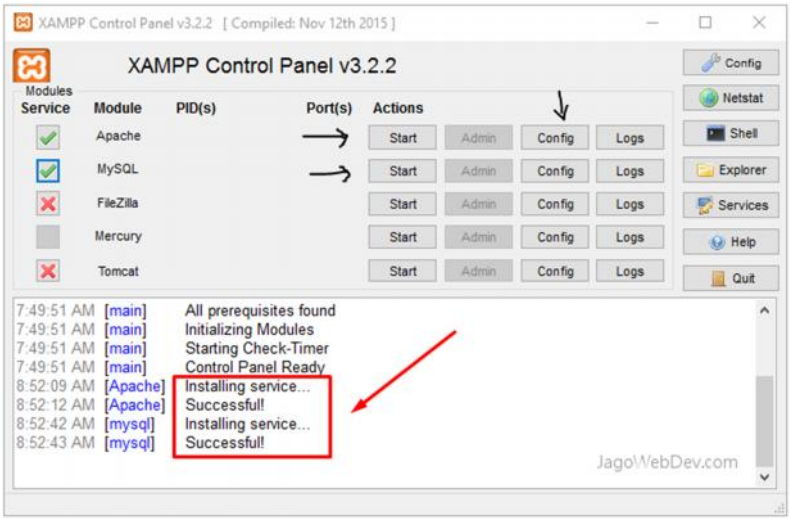
2. Pengumpulan alat dan bahan

   Pengumpulan alat dan bahan pada penelitian ini meliputi laptop sebagai alat untuk menjalankan *software* yang dibutuhkan seperti XAMPP v3.2.2, Chrome Web Browser, dan Winbox-2.2.16. Pengumpulan alat dan bahan yang lain meliputi Router Firewall 1 buah, yang difungsikan sebagai gateway dari server ke client, serta sebagai firewall untuk menjalankan fungsi translasi PAT (Port Address Translation) dari client ke server dan Kabel UTP 1 meter 2 buah dengan spesifikasi minimal cat 5.

3. Perancangan sistem jaringan meliputi Server dan Client

   a. Perancangan Server

      Server diinstallkan aplikasi webserver XAMPP v3.2.2 serta script html berupa informasi yang akan di tampilkan di PC client sebagai informasi. Buka aplikasi XAMPP dan atur Control Panel untuk memulai / menghentikan service web dengan mengklik Start pada Apache dan MySql sampai dengan mengganti port web server dari default 80 menjadi 99 pada item config.



Gambar 3.2 XAMPP Control Panel v3.2.2

1. Server disetup IP Address private 192.168.1.2/30 dengan gateway 192.168.1.1, dimana /30 disini adalah subnet mask 255.255.255.252, artinya ada 2 host yang dapat terhubung dalam 1 network yaitu server dan router firewall.
2. Router firewall disetupkan IP Address private kearah server (port 2) 192.168.1.1/30, serta disetupkan IP Address public kearah client (port 1) dengan IP Address 202.152.5.1/29, dimana /29 disini adalah subnetmask 255.255.255.248, artinya ada 6 host yang dapat terhubung dalam 1 network ke router firewall. Disamping itu configure wlan dengan SSID wifi-kampus dengan DHCP server 202.152.5.3/32 yang di bridge dengan port 1 sehingga sisi client dapat mengakses baik menggunakan kabel UTP (keport 1), maupun dengan menggunakan wifi yang terkoneksi ke SSID wifi-kampus.

b. Perancangan Client

1 PC Client 1 (Laptop) disetupkan IP Address public 202.152.5.2/29 dengan subnetmask 255.255.255.248 dengan default gateway 202.152.5.1

2 Client 2 (Smartphone) diaktifkan WIFI nya dengan menangkap SSID wifi-kampus sampai dengan status connected dan mendapatkan IP Address DHCP 202.152.5.3

3 Hubungkan kabel UTP dari server (Port Ethernet) ke Router Firewall port 2

4 Hubungkan kabel UTP dari Router Firewall port 1 ke PC Client 1 (Laptop)

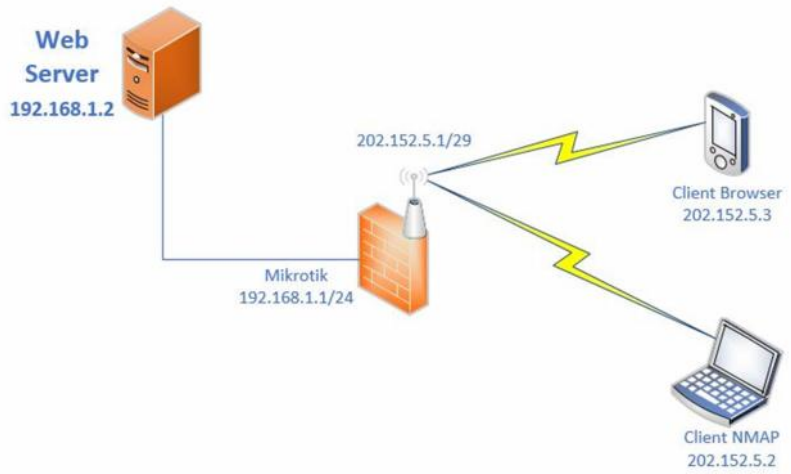
5 Pastikan Server dapat melakukan ping test lewat command prompt ke ip 192.168.1.1, jika statusnya reply maka sudah terhubung, jika request timed out maka masih terputus.

6 Pastikan dari PC Client 1 (Laptop) dapat melakukan ping test lewat command prompt ke ip router firewall 202.152.5.1, jika statusnya reply maka sudah terhubung, jika request timed out maka masih terputus.

7 Pastikan dari Router Firewall dapat melakukan ping test lewat aplikasi winbox >> terminal monitor ke ip address smartphone 202.152.5.3, jika statusnya reply maka sudah terhubung, jika request timed out maka masih terputus.

c. Pembandingan hasil metode Port Address Translation dan metode Packet Filtering.

Pengukuran dilakukan dengan mengambil log data hasil traffic menggunakan aplikasi Winbox dari laptop server yang berisi informasi tentang kecepatan dan besar data yang lewat dari apa yang diakses dalam hal ini web server. Metode pengambilan log menggunakan tiga kondisi yaitu pada kondisi normal, dihack, dan full traffic dengan menggunakan teknik packet filtering dan teknik port address translation (PAT).



Gambar 3.3 Blok Diagram Perancangan Jaringan PAT

Setelah didapatkan log hasil traffic dari kedua metode tersebut, selanjutkan dilakukan perbandingan antar keduanya terhadap faktor-faktor yang dapat menjadi celah dalam menilai webserver tersebut aman dari serangan atau tidak.

F. Teknik Analisis Data

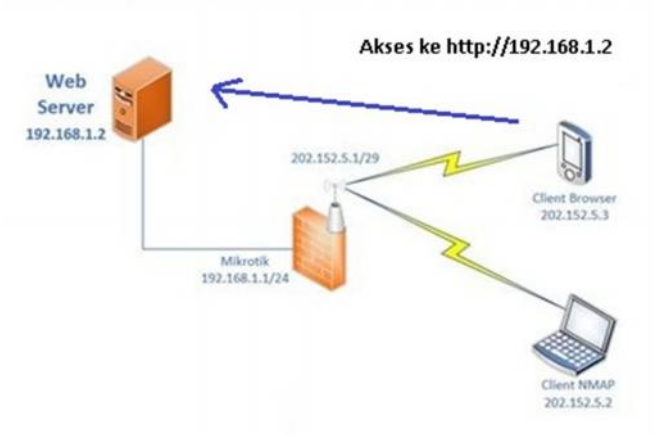
Teknik analisis terhadap data yang diperoleh adalah melalui analisa deskriptif yaitu menjelaskan data hasil pengambilan log melalui metode packet filtering dengan metode port address translation (PAT), Data hasil perbandingan disajikan dalam bentuk log (tampilan) traffic dari aplikasi Winbox untuk masing-masing kondisi yang digunakan diantaranya kondisi normal, dihack, dan full traffic. Log tersebut menunjukkan adanya perbandingan celah keamanan yang diperlihatkan dari webserver yang dapat menjadi keuntungan bagi pihak yang tidak bertanggung jawab.

BAB IV

HASIL DAN PEMBAHASAN

A. Analisa Metode Packet Filtering

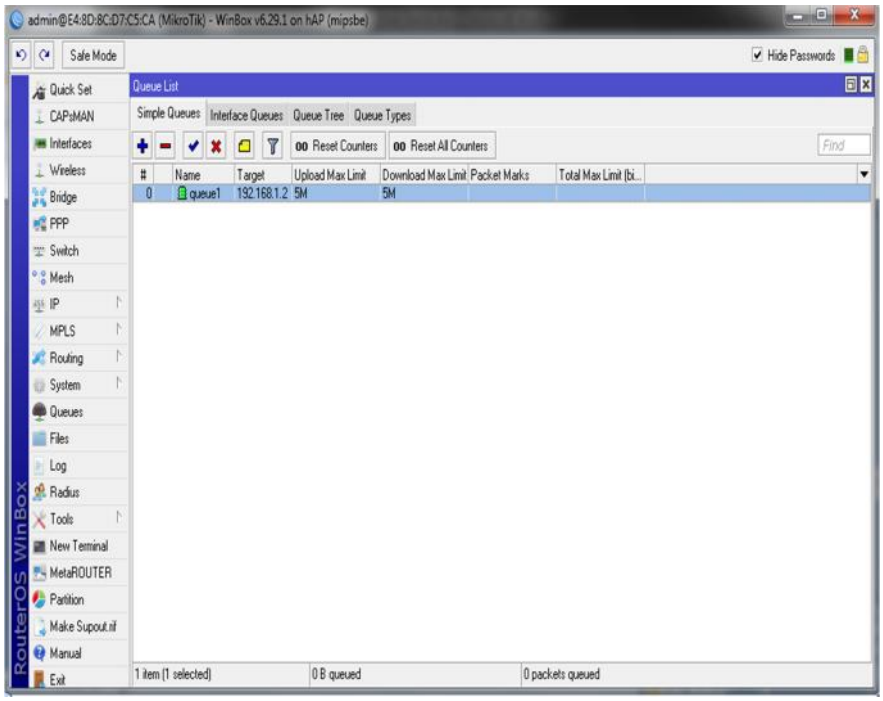
Pada tahap ini akan di analisa metode firewall yang sering digunakan secara umum dalam pemfilteran satu layer, salah satunya adalah menggunakan metode *Firewall Packet Filtering,* firewall jenis ini memfilter paket data berdasarkan alamat dan opsi-opsi yang sudah ditentukan untuk paket tersebut. Metode ini bekerja dalam level IP paket data dan membuat keputusan mengenai tindakan selanjutnya (diteruskan atau tidak diteruskan) berdasarkan kondisi paket tersebut. metode ini di desain untuk mengontrol aliran paket berdasarkan alamat asal, tujuan, port dan tipe informasi paket yang dikandung di dalam tiap paket.



Gambar 4.1 Skema Paket Filtering

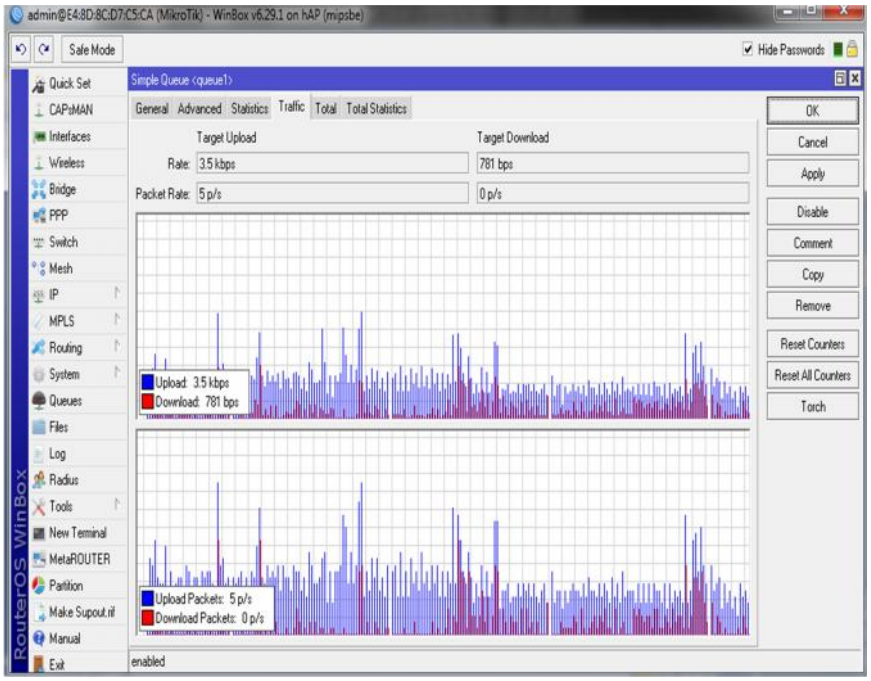
Ketika paket masuk melewati firewall, paket filter akan langsung menginspeksi header setiap paket, kemudian mencocokan dengan kebijakan dan peraturan yg diterapkan pada paket filter, paket akan lewat jika memang di izinkan, sedangkan paket akan di tolak apabila paket tersebut tidak memenuhi syarat pada paket filter.

1. Pengujian metode paket filtering pada kondisi normal:



Gambar 4.2 Tampilan menu simple Queues

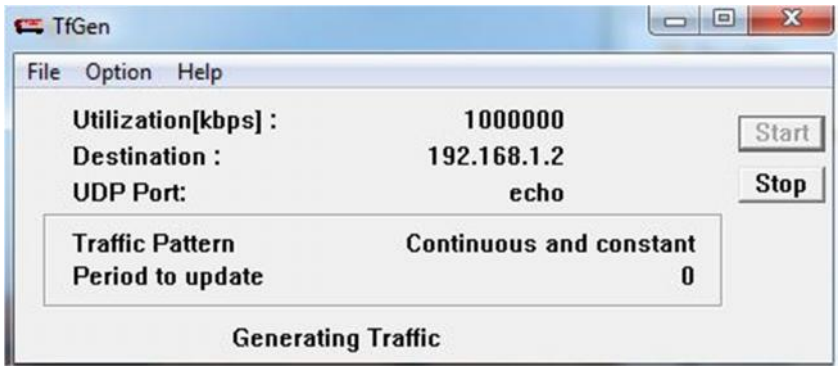
Gambar 4.2 menunjukkan indicator warna hijau pada queues yang berarti dalam kondisi normal.



Gambar 4.3 Tampilan winbox menu simple Queues Traffic

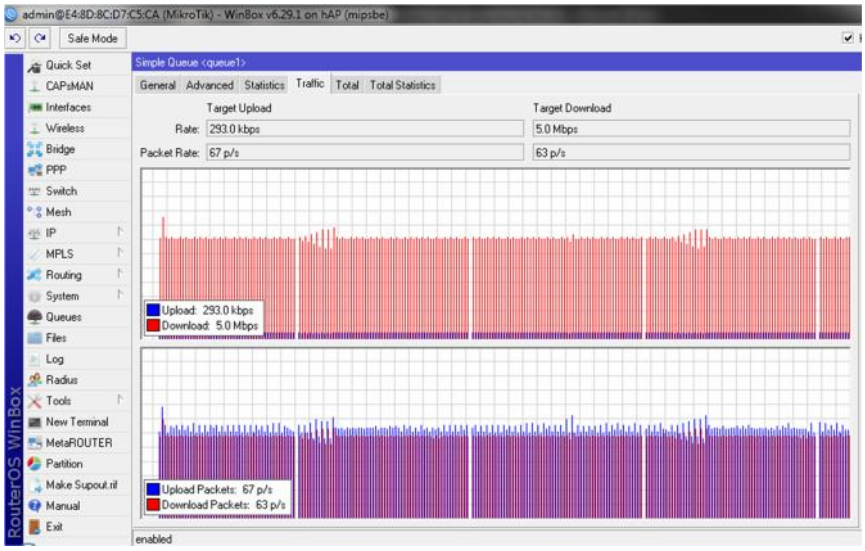
Gambar 4.3 menunjukkan traffic yang yang lewat yaitu traffic upload (warna biru) sebesar 3.5kbps dan Download (warna merah) sebesar 781bps. Dalam kondisi normal terdapat traffic dalam jumlah kecil dimana traffic tersebut menunjukkan aktifitas lalu lintas data pada jaringan server berupa broadcast ip yang berasal dari client ke tujuan (server) sehingga terlihat masih ada sedikit traffic data dan memungkinkan terjadinya transfer virus dan sejenisnya.

2. Pengujian metode paket filtering pada kondisi di hack :



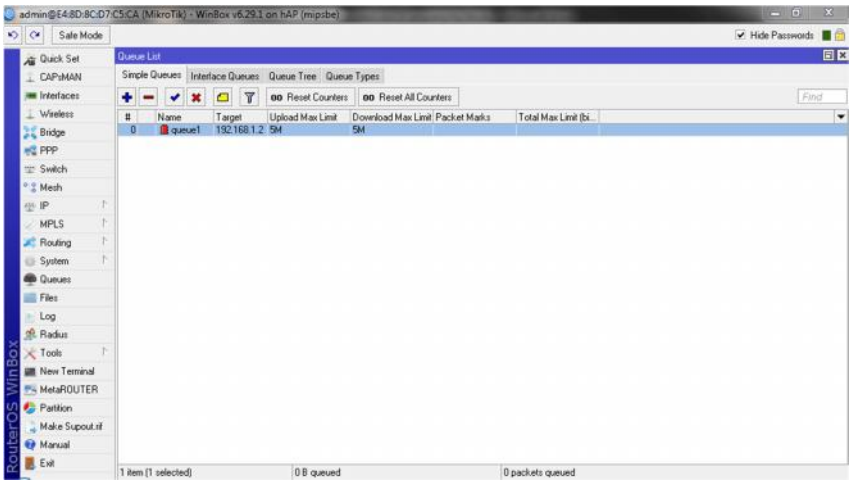
Gambar 4.4 Tampilan TFGen

Gambar 4.4 menunjukkan tampilan aplikasi TFGen, dimana dilakukan hacking data sebesar 1jt kbps kearah server 192.168.1.2



Gambar 4.5 Tampilan winbox menu simple Queues Traffic

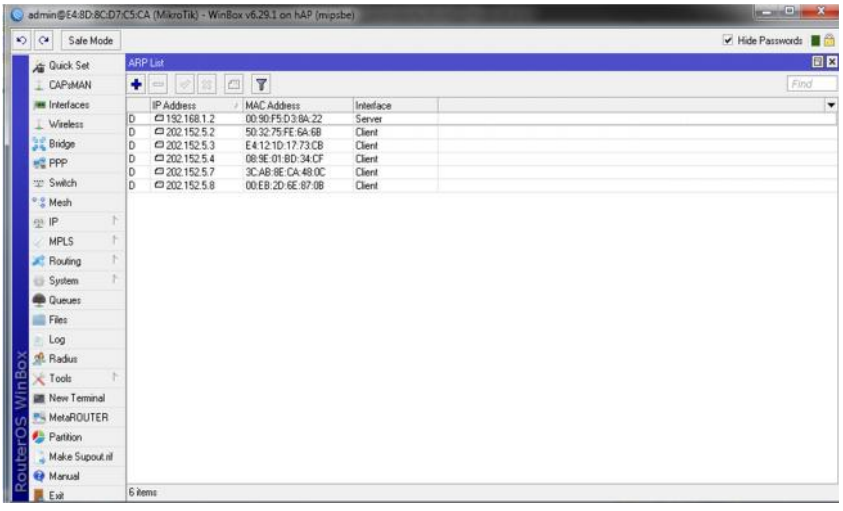
Gambar 4.5 merupakan tampilan winbox menu simple Queues Traffic menggunakan metode Paket Filter, dimana traffic Upload 293kbps dan download 5Mbps yang berarti traffic memenuhi jaringan kearah server sehingga server sulit untuk diakses.



Gambar 4.6 Tampilan menu simple Queues

Pada gambar 4.6 Tampilan menu simple Queues menunjukkan indicator Traffic berwarna merah yang berarti traffic dalam kondisi full akibat terkena serangan.

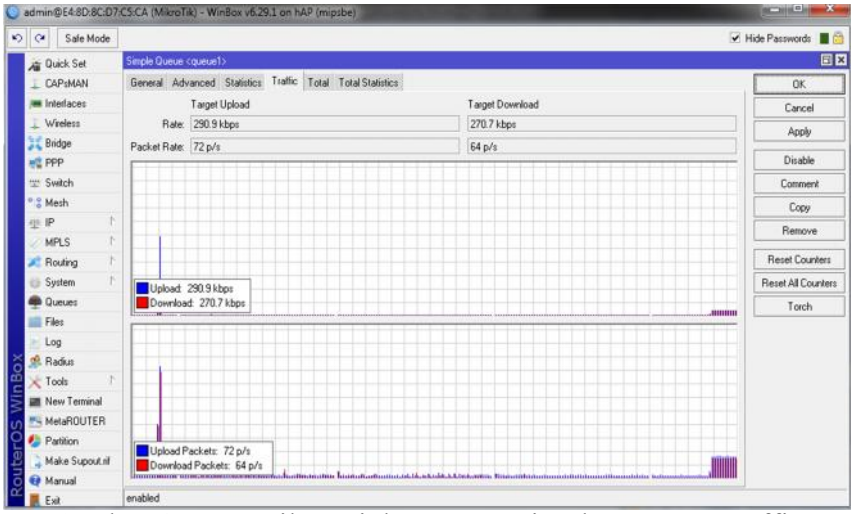
3. Pengujian metode paket filtering pada kondisi Full Akses :



Gambar 4.7 Tampilan menu IP ARP List

Gambar 4.7 menunjukkan jumlah IP Server dan IP Client yang terhubung ke satu jaringan dimana pada Gambar 4.7

menampilkan 1 IP Server dan 5 IP Client yang terkoneksi ke server.

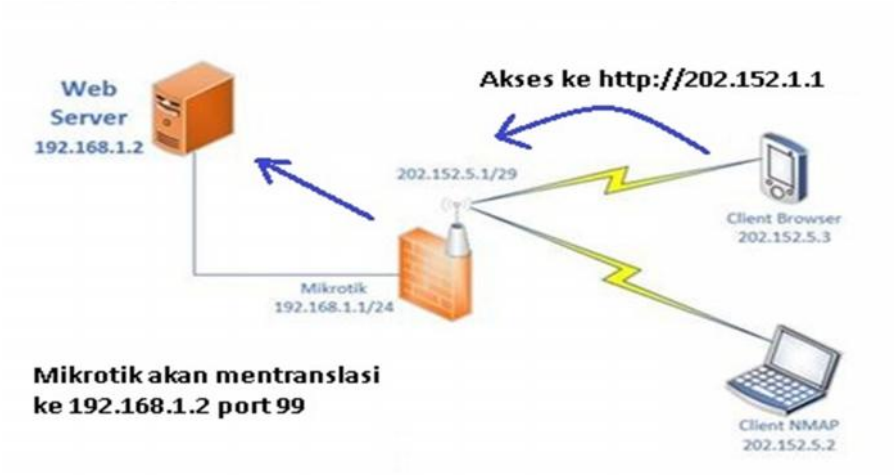


Gambar 4.8 Tampilan winbox menu simple Queues Traffic

Gambar 4.8 merupakan tampilan winbox menu simple Queues Traffic menggunakan metode Paket Filter, dalam kondisi full traffic yang menunjukkan data upload 290,9kbps dan download 270,7kbps yang berarti disamping akses data yang dilakukan oleh banyak client ke server juga broadcast dan kemungkinan virus dapat juga mengisi traffic data kearah server.

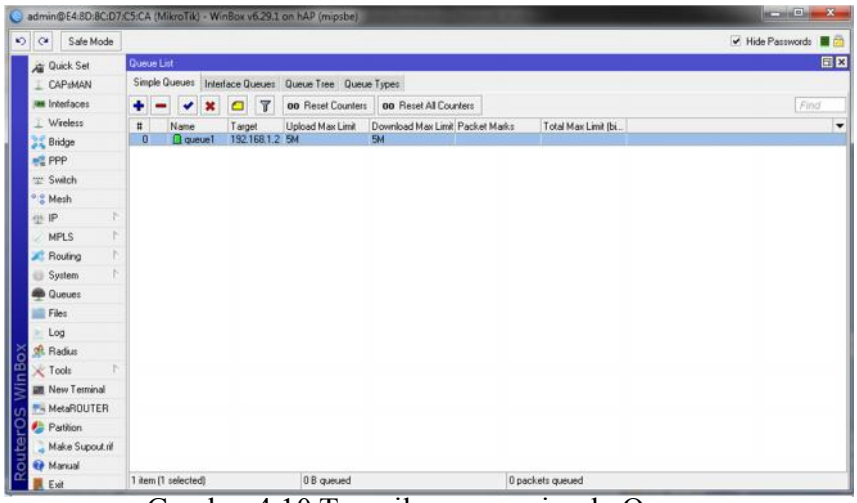
B. Analisa Metode Port Address Translation

Pada tahap berikutnya akan di analisa metode firewall lainnya yaitu port address translation (PAT), metode firewall jenis ini memanfaatkan Router OS sebagai gateway PAT serta mewakili ip serta port webserver yang akan diakses oleh client.



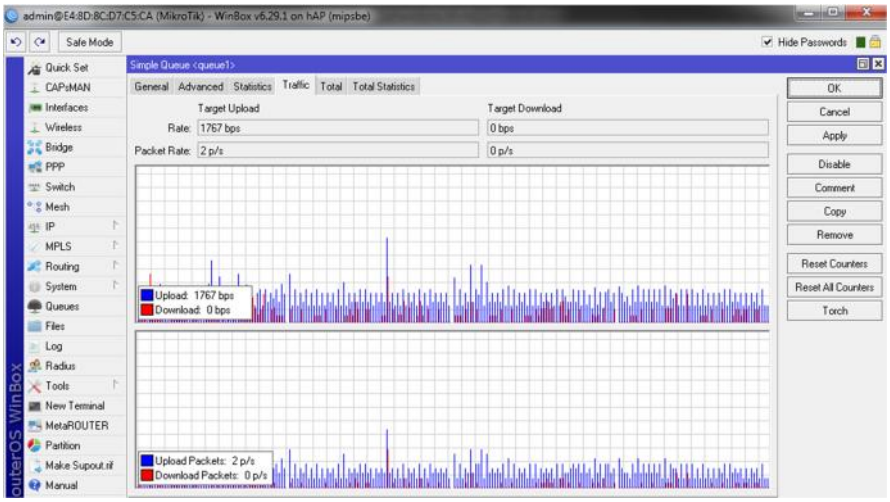
Gambar 4.9 Skema Sistem Port Address Translation

1. **Pengujian metode port address translation pada kondisi normal:**



Gambar 4.10 Tampilan menu simple Queues

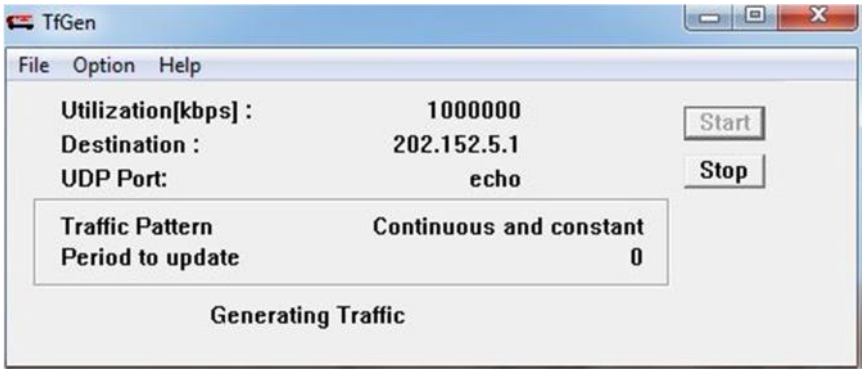
Gambar 4.10 menunjukkan indicator warna hijau pada queues yang berarti dalam kondisi normal.



Gambar 4.11 Tampilan winbox menu simple Queues Traffic

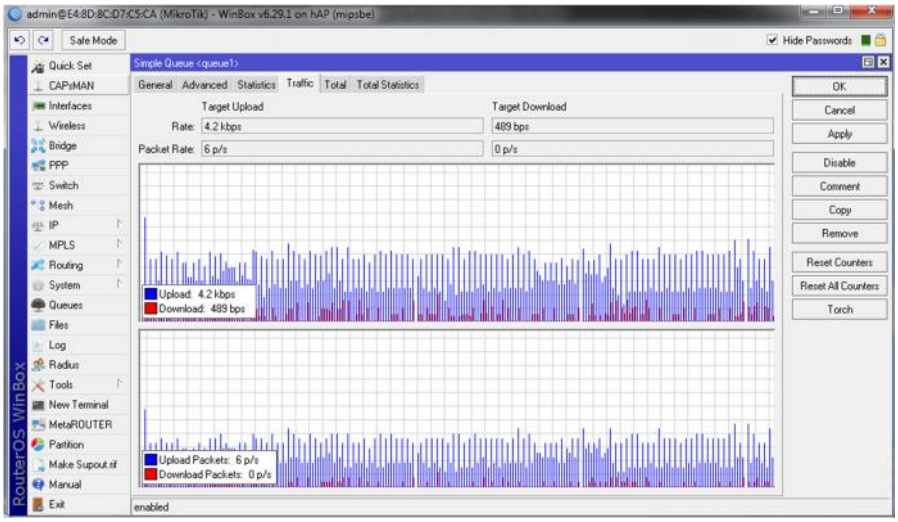
Gambar 4.11 menunjukkan traffic yang yang lewat yaitu traffic upload (warna biru) sebesar 1767bps dan Download (warna merah) sebesar 0bps. Dalam kondisi normal terdapat traffic dalam jumlah kecil dimana traffic tersebut menunjukkan aktifitas lalu lintas data pada jaringan server berupa broadcast yang terjadi antara server ke mikrotik dan client ke mikrotik disebabkan tidak adanya koneksi secara langsung sehingga traffic yang terlihat sangat kecil bahkan tidak ada.

2. Pengujian metode port address translation pada kondisi di hack:



Gambar 4.12 Tampilan TFGen

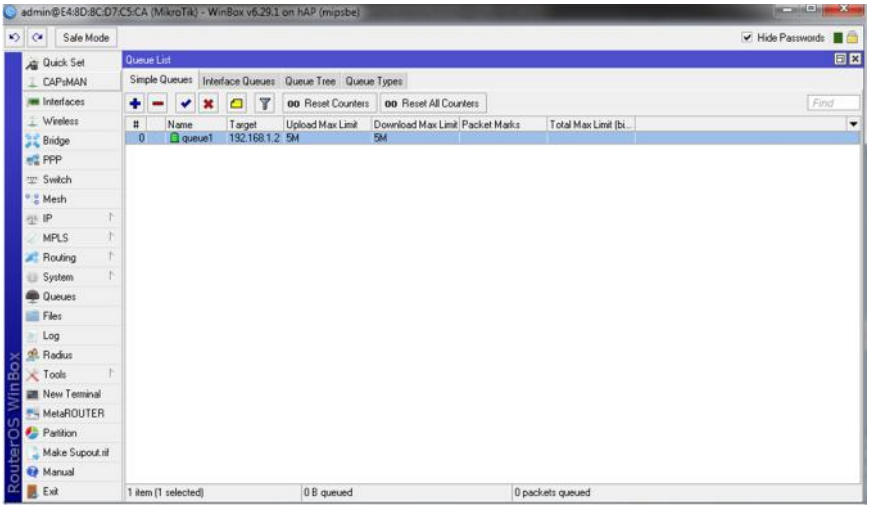
Pada Gambar 4.12 menunjukkan serangan menggunakan aplikasi TFGen,dimana dilakukan hacking data sebesar 1jt kbps kearah server 202.152.5.1.



Gambar 4.13 Tampilan winbox menu simple Queues Traffic

Gambar 4.13 merupakan tampilan winbox menu simple Queues Traffic menggunakan metode port address translation,

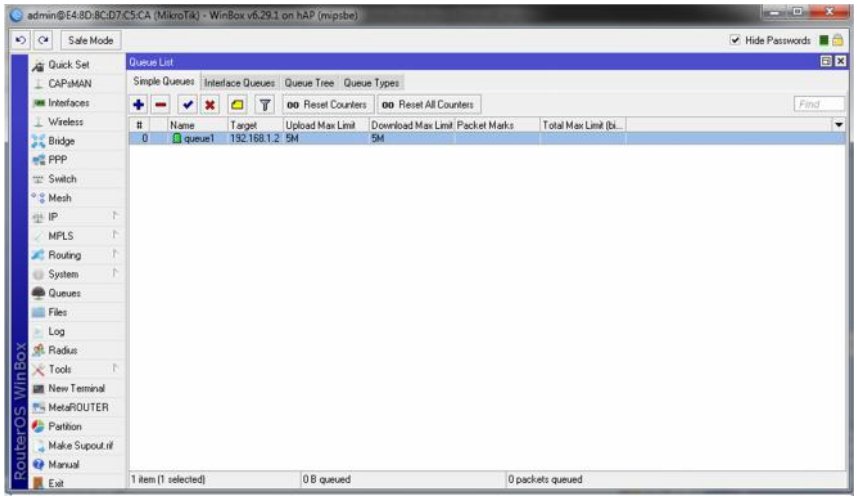
dimana traffic yang muncul tidak terlalu besar kearah server yaitu upload 4,2kbps dan download 489bps.



Gambar 4.14 Tampilan menu simple Queues

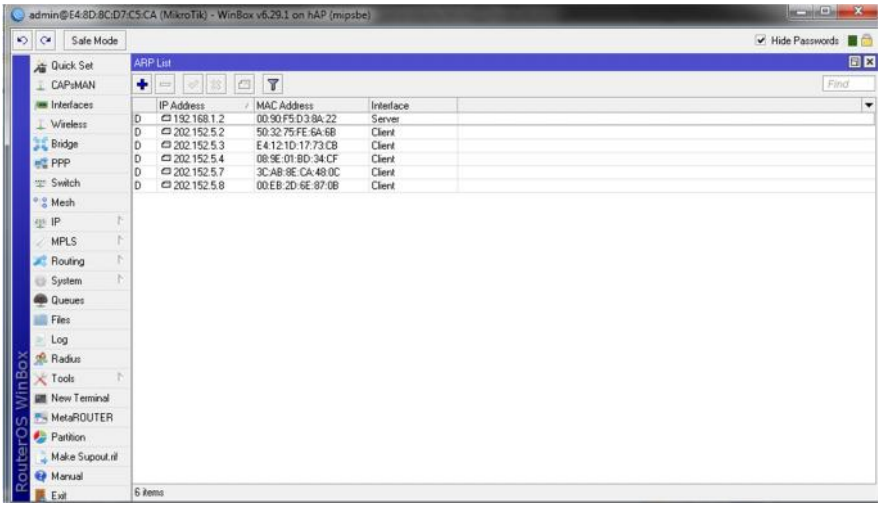
Gambar 4.14 menunjukkan indicator warna hijau pada queues yang berarti dalam kondisi normal pada saat di hack berarti serangan tidak berdampak pada jaringan server sehingga walaupun dalam kondisi dihack tidak akan berdampak pada client yang mengakses ke server.

3. Pengujian metode port address translation pada kondisi full akses:



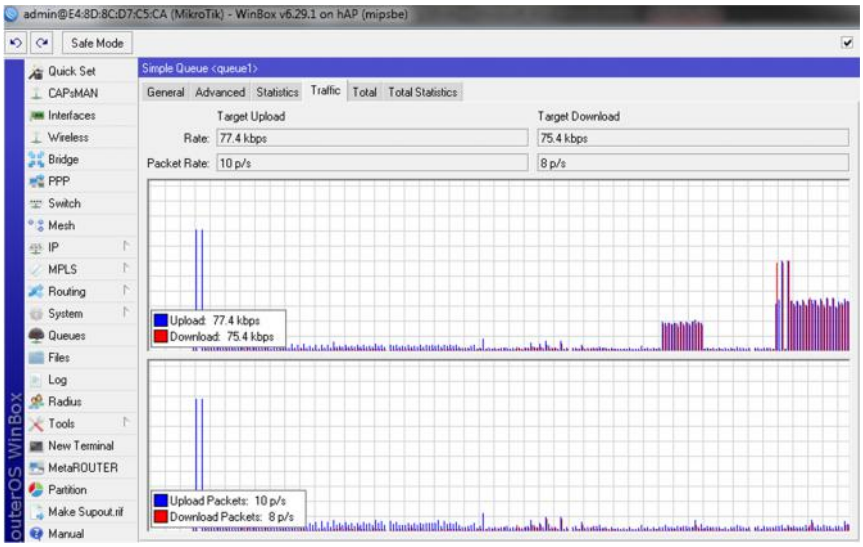
Gambar 4.15 Tampilan menu simple Queues

Gambar 4.15 menunjukkan indicator warna hijau pada queues yang berarti dalam kondisi normal pada saat di hack.



Gambar 4.16 Tampilan menu IP ARP List

Gambar 4.16 menunjukkan jumlah IP Server dan IP Client yang terhubung ke satu jaringan dimana pada Gambar 4.16 menampilkan 1 IP Server dan 5 IP Client yang terkoneksi ke server.



Gambar 4.17 Tampilan winbox menu simple Queues Traffic

Gambar 4.17 merupakan tampilan winbox menu simple Queues Traffic menggunakan metode port address translation, dalam kondisi full traffic yang menunjukkan data upload 77,4kbps dan download 75,4kbps yang berarti traffic yang muncul berasal dari client ke server hanya murni data saja yang lewat sehingga traffic yang muncul adalah traffic yang sebenarnya.

C. Perbandingan Analisa Metode Packet Filtering dan Metode Port Address Translation

Berdasarkan dua metode diatas, jika menggunakan metode pemfilteran paket filtering biasa, kemungkinan besar akan meloloskan paket data yang sebenarnya sehingga membahayakan segmen jaringan *local area network* yang terdapat pada webserver, dengan demikian walaupun menggunakan metode *firewall packet filtering* sudah baik, tetapi dilihat dari metode inspeksi yang digunakan, masih terdapat kekurangan dalam melakukan inspeksi terhadap paket data pada lalu lintas jaringan, sehingga perlu dilakukan pemfilteran secara selektif, agar dalam pemfilteran paket yang melalui lalu lintas firewall, akan benar-benar terinspeksi secara selektif, disamping menghasilkan sisi kemudahan dalam membaca informasi *log* dan fungsionalitas sistem firewall, baik itu dilihat dari metode ataupun sistem yang digunakan, maka perlu ditingkatkan lagi.

Sedangkan pada metode port address translation (PAT), dalam hal ini memanfaatkan Router OS sebagai gateway PAT serta mewakili ip webserver yang akan diakses oleh client dimana koneksi bisa dilakukan ke webserver tanpa harus mengakses IP yang terdapat pada webserver sesungguhnya, dengan kata lain IP webserver dialiaskan menggunakan ip yang terdapat pada perangkat mikrotik firewall. Adapun kekurangan PAT dibandingkan paket filter adalah protocol yang dapat ditranslasikan oleh metode PAT hanya protocol TCP sedangkan protocol lain seperti UDP (voice / video) dan ICMP (ping) tidak dapat ditranslasikan sedangkan dengan metode packet filter hal itu dapat dilakukan tanpa kendala.

BAB V

PENUTUP

H. Kesimpulan

Dari keseluruhan hasil pengujian dan analisis pada penelitian tugas akhir ini, dapat diperoleh kesimpulan :

1. Dengan menggunakan metode Port Address Translation, alamat ip address yang sebenarnya terdapat pada webserver tidak akan pernah terdeteksi oleh client sehingga aman secara jaringan dan serangan hacker. Hal ini di buktikan dengan analisa perbandingan traffic saat kondisi terjadi serangan pada packet filter dan kondisi serangan pada metode PAT.
2. Dengan menggunakan metode Packet Filtering, metode inspeksi yang digunakan, masih terdapat kekurangan dalam melakukan inspeksi terhadap paket data pada lalu lintas jaringan, sehingga perlu dilakukan pemfilteran secara selektif, agar dalam pemfilteran paket yang melalui lalu lintas firewall, akan benar-benar terinspeksi secara selektif, disamping menghasilkan sisi kemudahan dalam membaca informasi *log* dan fungsionalitas sistem firewall, baik itu dilihat dari metode ataupun sistem yang digunakan, maka perlu ditingkatkan lagi.

I. Saran

Metode Port Address Translation yang diterapkan pada Mikrotik Router OS ini masih memerlukan pengembangan keamanan untuk menangani keamanan pada segmen aplikasi dengan menggunakan metode IPS (Instrusion Prevention System). Yang mana dapat melakukan filtering tidak hanya dari sisi protocol port (layer transport), tapi sampai dengan layer aplikasi, dimana saat ini dengan perkembangan teknologi yang makin canggih, memungkinkan serangan dapat terjadi dari mana saja dan kapan saja. Dari semua kemungkinan tidak hanya pada transport layer (port), tapi sudah sampai ke layer aplikasi.

DAFTAR PUSTAKA

http://id.wikipedia.org/wiki/Tembo k_api#Stateful_Firewall, diupdate tanggal 11 juli 2013.

http://wiki.mikrotik.com/wiki/Fire wall, diupdate tanggal 5 April 2013.

http://wiki.mikrotik.com/wiki/Dmit ry_on_firewalling, diupdate tanggal 5 Mei 2009.

http://www.forummikrotik.com/ge neral-networking/15268-about- firewall.html, diupdate tanggal 24 Oktober 2010.

Imam. C (2013). *Linux Networking,* Penerbit Jasakom, Jakarta.

Janner Simarmata (2008). *Pengamanan Sistem Komputer*, Penerbit Andi. Yogyakarta.

Jusak. (2013). *Teknologi Komunikasi Data Modern,* Penerbit Andi. Yogyakarta.

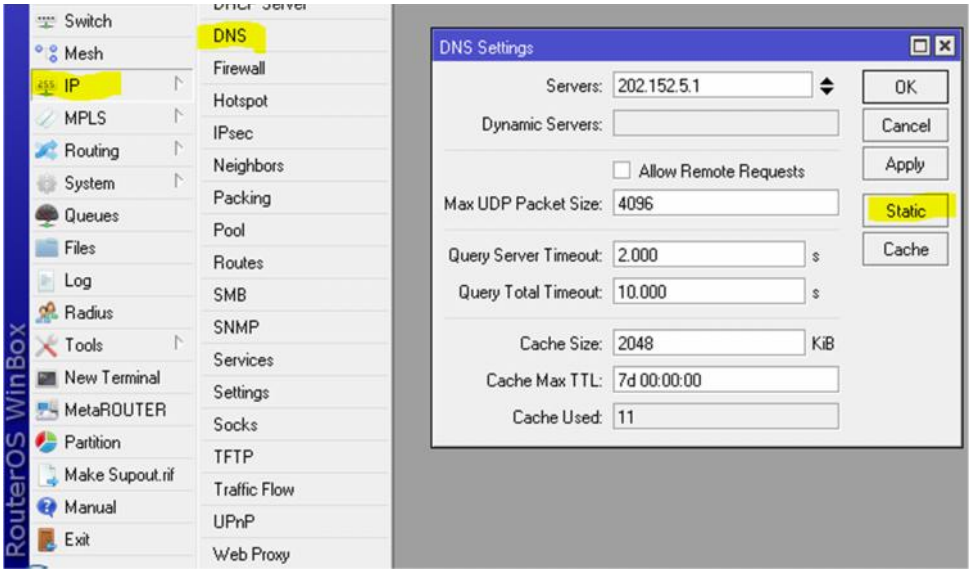
Onno W. Purbo (2008). *Keamanan Jaringan Internet,* Penerbit PT Elex Media Komputindo. Jakarta.

Shaymaa W. Abdulatteef, 2012. "An Implementation Of Firewall System Using Mikrotik Router OS". *Journal of university of anbar for pure science* Vol.6,Vol.2 , 8-11.

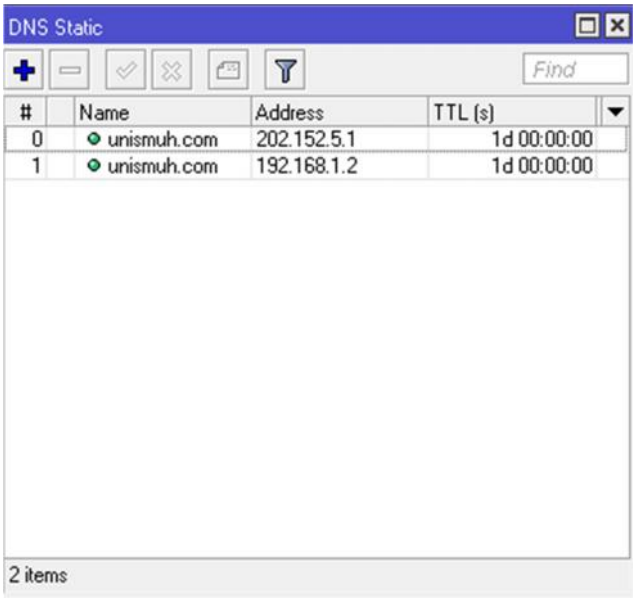
L A M P I R A N

LAMPIRAN

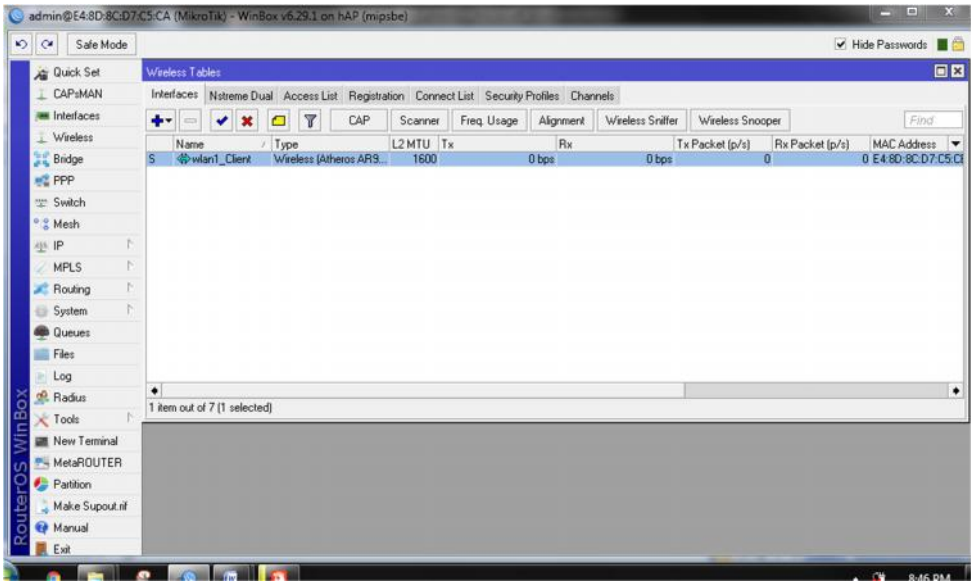
Lampiran 1 Tampilan DNS Settings Server



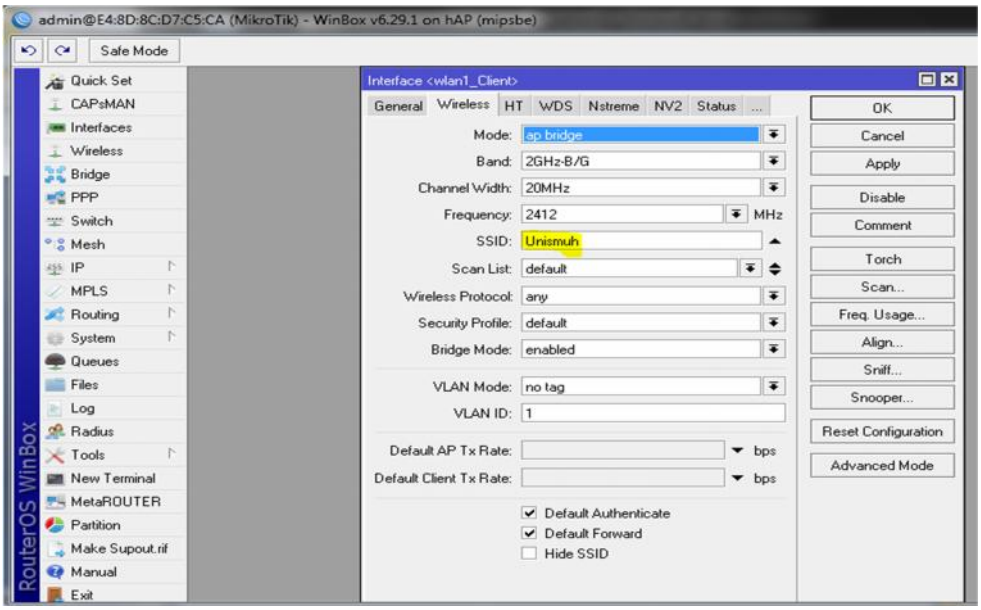
Lampiran 2 Tampilan Setting DNS Static



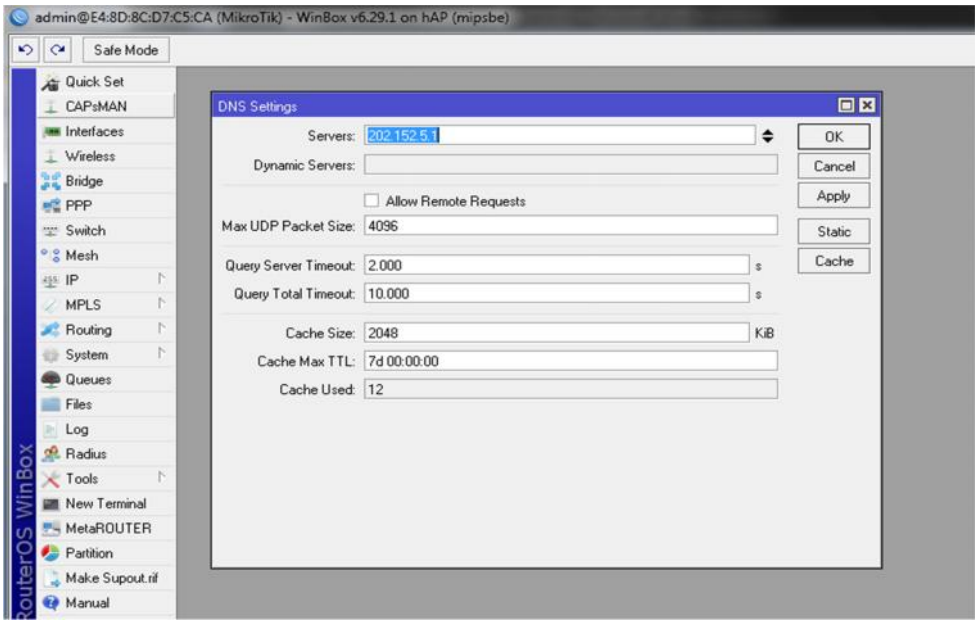
Lampiran 3 Tampilan SSID Wifi



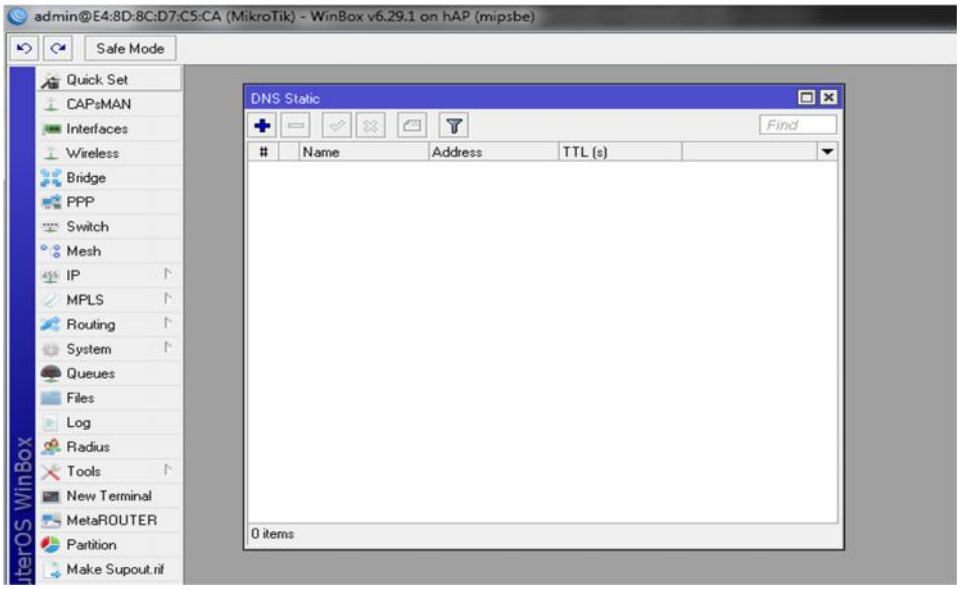
Lampiran 4 Tampilan Setting Domain IP



Lampiran 5 Tampilan DNS Setting Server



Lampiran 6 Tampilan DNS Static



Lampiran 7 Tampilan DNS Static Entry