Mapel : Administrasi Infrastruktur Jaringan
Guru : Ahmad Rifai, S. Kom
Kelas : XII TKJ

MATERI

Kompetensi Dasar:

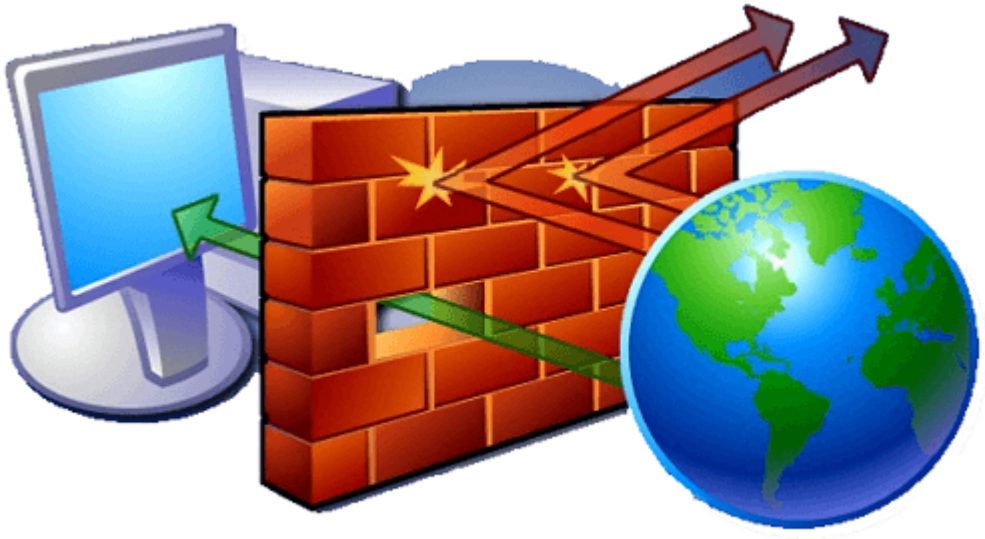
- Mengevaluasi Firewall Jaringan
- Mengkonfigurasi Firewall Jaringan

FIREWALL JARINGAN

Di era internet yang semakin canggih ini, setiap komputer dapat terhubung dengan komputer lainnya secara mudah. Pertukaran file atau dokumen pun semakin tanpa batas dan dapat dilakukan oleh siapa saja. Tentunya hal ini membawa dampak positif yang juga diiringi dengan dampak negatif.
Positifnya, orang semakin dimudahkan untuk berbagi berbagai dokumen yang diperlukan. Namun negatifnya, tidak semua orang berbagi dengan tujuan baik. Beberapa berusaha untuk menyerang komputer sebagai hacker, memata-matai (spionase) komputer tertentu demi kepentingan pribadi, atau bahkan mencuri data yang ada dalam suatu komputer.

Untuk mencegah dampak negatif tersebut, dibutuhkan *firewall* sebagai pengatur sistem komunikasi antara dua buah jaringan. Pada artikel di bawah ini, akan dijelaskan secara lengkap mengenai pengertian firewall,

Pengertian Firewall



Firewall dapat didefinisikan sebagai sistem yang didesain khusus untuk mencegah akses mencurigakan masuk ke dalam jaringan pribadi. Firewall sendiri dapat berupa perangkat keras atau perangkat lunak, bisa juga terdiri dari kombinasi keduanya.

Firewall (tembok penahan api) sendiri sebetulnya terinspirasi dari benda fisik bernama firewall yang dipasang di gedung-gedung untuk mencegah menjalarnya api dari sumbernya. Firewall untuk gedung banyak dipasang misalnya di kompleks-kompleks apartemen. Untuk memisahkan dua unit apartemen, dipasanglah sebuah firewall sehingga jika terjadi kebakaran api tidak dengan cepat menjalar dari satu unit ke unit lainnya.

Karena firewall berfungsi sebagai pembatas dengan dunia luar, maka untuk satu unit apartemen yang memiliki empat sisi misalnya, harus memasang firewall di keempat titik perbatasan. Jika salah satu sisi tidak dibatasi dengan firewall sementara ketiga sisi lainnya dipasangi firewall, maka akan sia-sia usaha menahan api yang akan menyebar dengan cepat. Begitu pula halnya dengan firewall untuk komputer.
Supaya dapat berfungsi secara efektif, sebuah firewall wajib memenuhi standar tertentu, mampu mendirikan suatu ‘pagar pengaman’ di sekeliling sebuah jaringan pribadi, mencegah masuknya akses tanpa izin dan berbagai gangguan terhadap dokumen atau file yang ada di komputer pengguna. Di pasaran, ada cukup banyak produk firewall yang ditawarkan dengan fungsi yang bervariasi. Perbedaan firewall satu dengan lainnya biasanya terdapat pada seberapa ketat pengamanan dan selektivitas akses, dan cakupan perlindungannya pada berbagai lapisan OSI (*Open System Interconnection*).

Fungsi Firewall

Firewall sebagai pos keamanan jaringan

Firewall sendiri memiliki beberapa fungsi untuk melindungi jaringan komputer yang dapat dijabarkan dalam beberapa poin berikut:

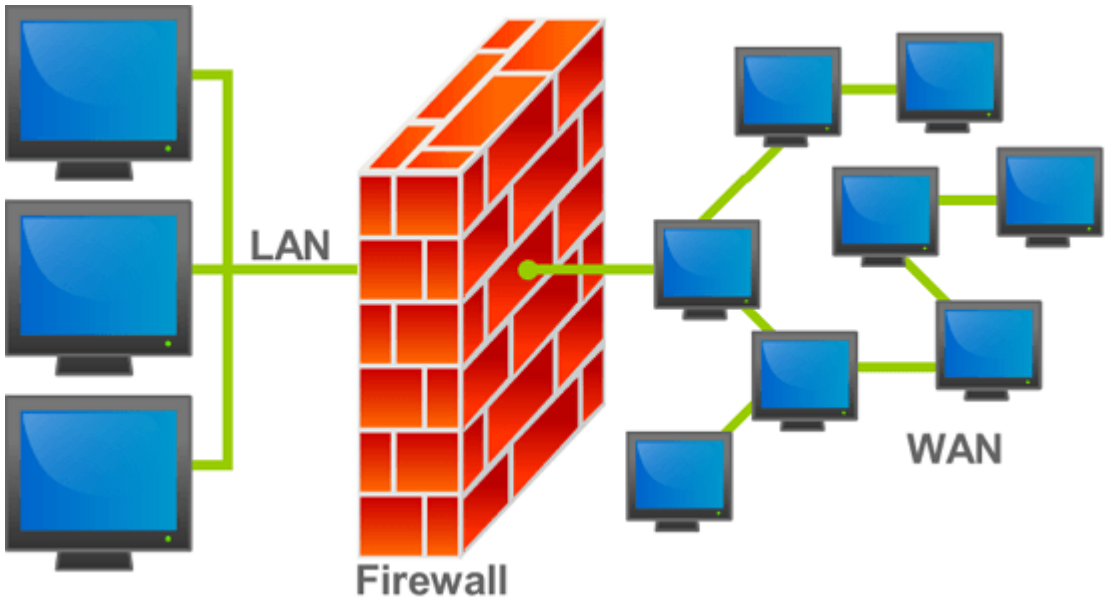
1. Sebagai Pos Keamanan Jaringan. Semua lalu lintas yang masuk atau keluar jaringan harus melalui firewall sebagai pos kemanan yang akan melakukan pemeriksaan. Setiap terjadi lalu-lintas, firewall akan berusaha menyaring agar lalu lintas sesuai dengan keamanan yang telah ditentukan.
2. Mencegah Informasi Berharga Bocor Tanpa Sepengatahuan. Untuk fungsi yang satu ini, firewall banyak dipasang untuk *File Transfer Protocol* (FTP), sehingga setiap lalu-lintas data dikendalikan oleh firewall. Dalam hal ini, firewall bermanfaat untuk mencegah pengguna di jaringan mengirim file berharga yang sifatnya konfidensial (rahasia) kepada pihak lain.
3. Mencatat Aktivitas Pengguna. Setiap kali akan mengakses data, pengguna jaringan akan melalui firewall yang kemudian mencatatnya sebagai dokumentasi (*log files*) yang di kemudian hari bisa dibuka catatannya untuk mengembangkan sistem keamanan. Firewall mampu mengakses data log sekaligus menyediakan statistik mengenai penggunaan jaringan.
4. Memodifikasi Paket Data yang Datang. Dikenal juga dengan istilah NAT (*Network Address Translation*). NAT digunakan untuk menyembunyikan sebuah IP adress, sehingga membuat para pengguna dapat mengakses internet tanpa IP adress publik, yang sering juga disebut dengan istilah *IP masquerading*.
5. Mencegah Modifikasi Data Pihak Lain. Misalnya dalam urusan bisnis untuk informasi laporan keuangan, spesifikasi produk, dan lainnya yang menjadi rahasia perusahaan dan akan berdampak negatif jika diketahui pihak lain. Firewall mencegah modifikasi data-data tersebut sehingga tetap berada dalam keadaan aman.

Ciri – Ciri Firewall

1. Firewall harus dapat lebih kuat dan tangguh terhadap serangan di luar. Hal ini artinya sistem operasi komputer akan lebih aman dan penggunaan sistem bisa diandalkan.
2. Yang dapat melakukan hubungan adalah aktivitas yang dikenal atau terdaftar pada jaringan. Dalam hal ini dilaksanakan dengan cara setting policy pada konfigurasi keamanan lokal.
3. Seluruh kegiatan yang asalnya dari dalam ke luar harus melalui firewall lebih dulu. Hal ini dilaksanakan dengan memberikan batasan atau meblokir setiap akses kepada jaringan lokal, terkecuali jika melalui firewall terlebih dahulu.

Cara Kerja Firewall

Pada dasarnya, firewall bekerja dengan cara membatasi komputer pribadi dengan internet. Firewall bekerja layaknya penjaga keamanan di depan gerbang rumah dan mengidentifikasi pengunjung yang datang, sekaligus menyaring penyusup yang berusaha memasuki komputer pribadi. Firewall bekerja seperti garda pertahanan terdepan untuk menahan segala



usaha *hacking* yang masuk ke dalam komputer.

Firewall melakukan filter terhadap data masuk yang berasal dari WAN (internet)

Teknologi firewall pun kian hari kian berkembang. Sebelumnya, firewall bekerja menyaring lalu lintas komputer dengan menggunakan alamat IP, nomor port, serta protokol. Seiring dengan perkembangannya, kini firewall mampu menyaring data yang masuk dengan mengidentifikasi terlebih dahulu pesan konten yang dibawanya. Untuk mengatur lalu-lintas perpindahan data komputer dan internet, firewall dapat menggunakan salah satu atau gabungan dari beberapa metode berikut :

1. Packet Filtering

Merupakan sebuah cara kerja firewall dengan memonitor paket yang masuk dan keluar, mengizinkannya untuk lewat atau tertahan berdasarkan alamat *Internet Protocol* (IP), protokol, dan portnya. Packet filtering biasanya cukup efektif digunakan untuk menahan serangan dari luar sebuah LAN. Packet filtering disebut juga dengan firewall statis.
Selama terjadinya komunikasi dengan jaringan internet, packet yang datang disaring dan dicocokkan dengan aturan yang sebelumnya telah dibuat dalam membangun firewall. Jika data tersebut cocok, maka data dapat diterima dan sebaliknya jika tidak cocok dengan aturan, maka data tersebut ditolak.

Dalam metode packet filtering, firewall mengecek sumber dan tujuan alamat IP. Pengirim packet mungkin saja menggunakan aplikasi dan program yang berbeda, sehingga packet filtering juga mengecek sumber dan tujuan protokol, seperti UDP (*User Datagram Protocol*) dan TCP (*Transmission Control Protocol*).

2. Inspeksi Stateful

Berkebalikan dengan *Packet Filtering*, Inspeksi Stateful dikenal pula dengan firewall dinamis. Pada inspeksi stateful, status aktif koneksi dimonitor, kemudian info yang didapatkan akan dipakai untuk menentukan apakah sebuah packet jaringan dapat menembus firewall.

Inspeksi stateful secara besar-besaran telah menggantikan packet filtering. Pada firewall statis, hanya header dari packet dicek, artinya seorang hacker dapat mengambil informasi melalui firewall dengan sederhana, yaitu mengindikasikan “reply” melalui header.

Sementara dengan firewall dinamis, sebuah packet dianalisis hingga ke dalam lapisan-lapisannya, dengan merekam alamat IP dan juga nomor portnya, sehingga keamanannya lebih ketat dibandingkan packet filtering. Jadi itulah pembahasan mengenai pengertian firewall, fungsi firewall, dan cara kerja firewall.

Konfigurasi firewall pada Mikrotik router

Firewall adalah sebuah sistem atau perangkat yang memberi otorisasi pada lalu lintas jaringan komputer yang dianggapnya aman untuk melaluinya dan melakukan pencegahan terhadap jaringan yang dianggap tidak aman. Firewall dapat berupa perangkat lunak (program komputer atau aplikasi) atau perangkat keras (peralatan khusus untuk menjalankan program

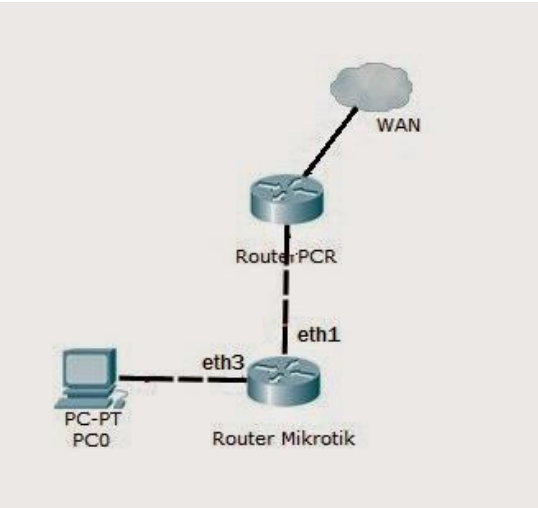
firewall) perangkat yang menyaring lalu lintas jaringan antara jaringan. Perlindungan dengn Firewall adalah mutlak diperlukan untuk komputasi perangkat seperti komputer yang diaktifkan dengan koneksi Internet. Meningkatkan tingkat keamanan jaringan komputer dengan memberikan informasi rinci tentang pola-pola lalu lintas jaringan. Perangkat ini penting dan sangat diperlukan karena bertindak sebagai gerbang keamanan antara jaring komputer internal dan jaringan komputer eksternal.

Fungsi firewall sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi Firewal mengatur, memfilter dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi, beberapa kriteria yang dilakukan fire-wall apakah memperbolehkan paket data lewati atau tidak, antara lain :

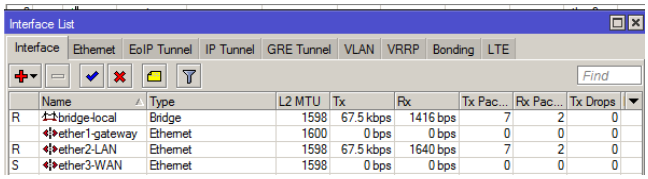
- Alamat IP dari komputer sumber
- Port TCP/UDP sumber dari sumber.
- Alamat IP dari komputer tujuan.
- Port TCP/UDP tujuan data pada komputer tujuan
- Informasi dari header yang disimpan dalam paket data.

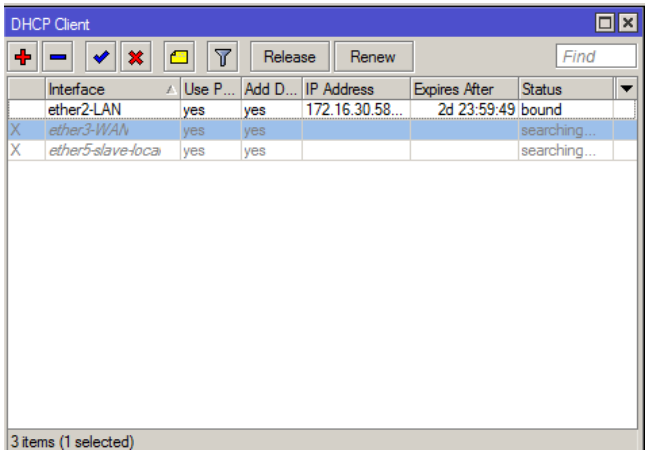
secara spesifik Fungsi Firewall adalah melakukan autentifikasi terhadap akses kejaringan. Applikasi proxy Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntutnya untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

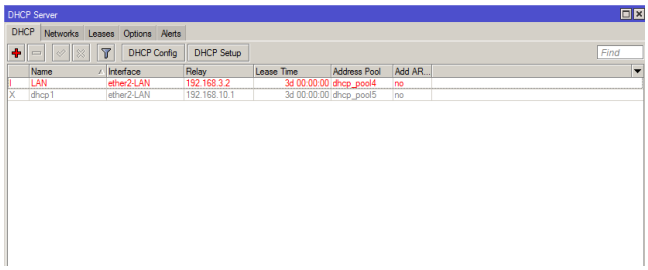
Pada kesempatan kali ini, akan dijelaskan tentang cara memblock user pada mikrotik dan juga mem-block beberapa situs yang tidak diinginkan untuk dibuka oleh user.
Adapun Topologi yang digunakan dalam percobaan ini ialah sebagai berikut :



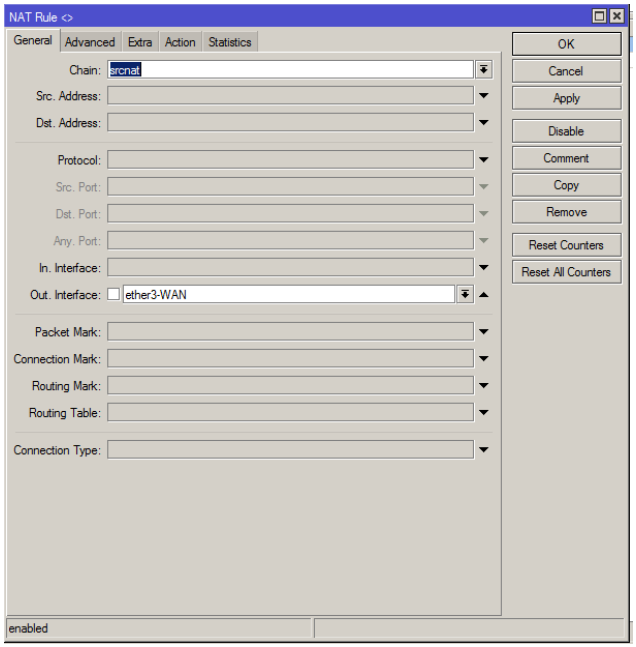
1. Jika sudah terhubung dengan benar, Buka aplikasi winbox pada pc yang terhubung ke mikrotik. Lalu klik *connect.*
*2. S*et mikrotik menjadi client bagi jaringan luar dan pc menjadi client dari mikrotiknya. sehingga Mikrotik mendapat IP dari jaringan luar, dalam hal ini adalah jaringan kampus PCR, dan PC mendapat IP yang disediakan oleh mikrotik.

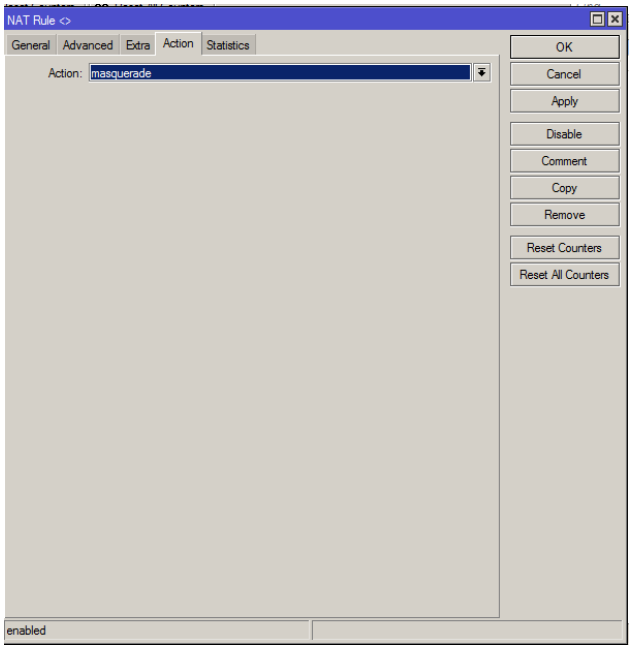




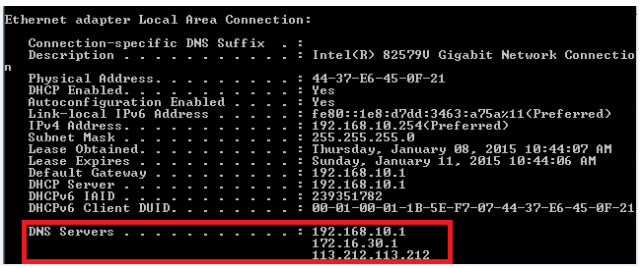


3. Atur konfigurasi NAT nya agar bisa terhubung ke jaringan luar,seperti yang telah kami jelaskan pada postingan sebelumnya

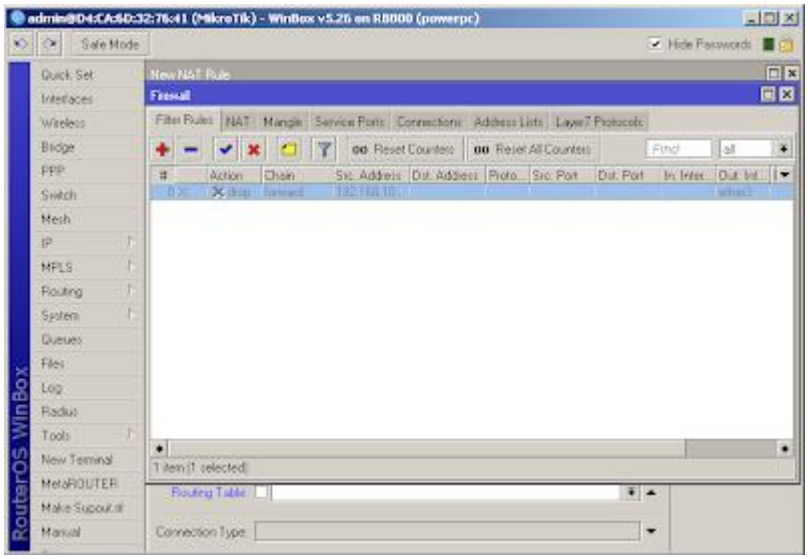




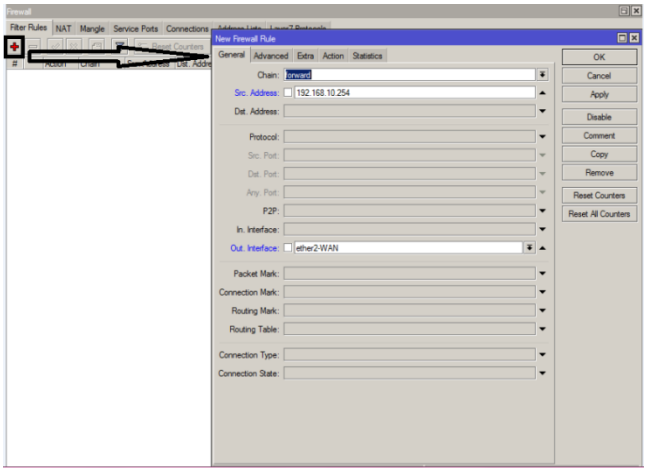
Maka kita akan mendapatkan ip dari mikrotik tersebut



4. Selanjutnya kita akan mencoba mem-block suatu IP, Klik **IP -> Firewall.** Lalu akan didapat tampilan seperti dibawah ini.

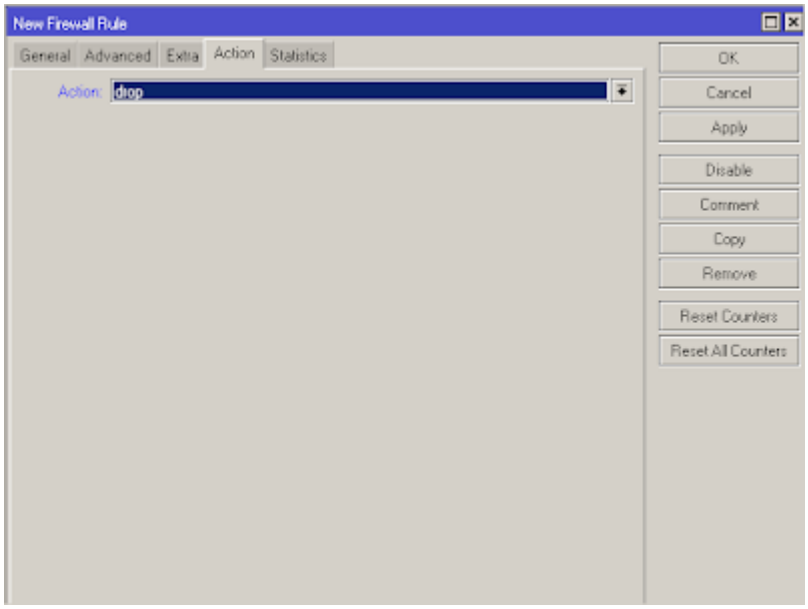


5. Pilih **Filter Rules** lalu klik tanda + yang berfungsi untuk menambahkan daftar block nya. Maka akan didapat tampilan seperti gambar dibawah:

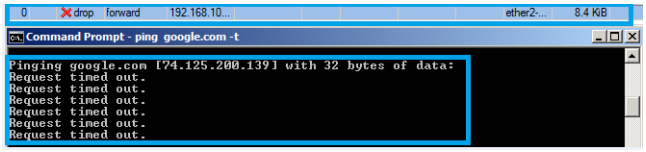


Pada bagian chain diisikan forward, yang mana digunakan untuk proses paket data yang melewati router.
Untuk out interface, disini kami menggunakan Ether 2, ini bisa diganti sesuai dengan ethernet mana yang digunakan untuk terhubung ke jaringan luar.

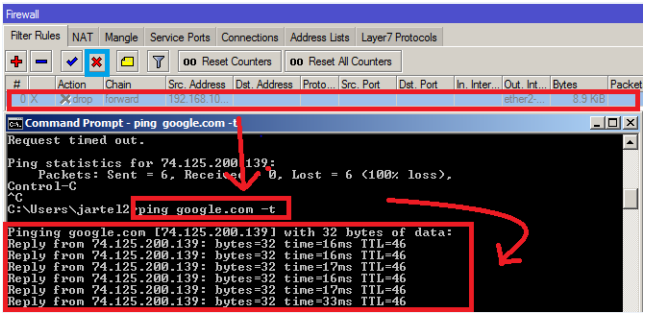
6. Lalu klik **action** , pilih **drop** yang berarti seluruh paket yang dikirim oleh PC client dengan IP yang telah didaftarkan akan di drop atau ditolak.



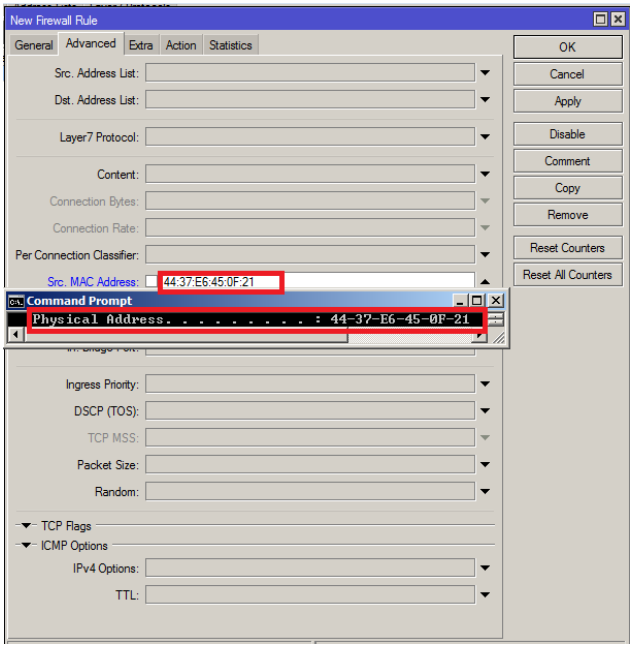
Dapat dibuktikan dengan tes PING ke ip yang diblock tersebut.



Apabila kita ingin menghapus block nya, kita cukup meng-klik tanda silang. contohnya sperti berikut



7. Selanjutnya, kita juga dapat memblok mac address dengan menggunakan mikrotik .Karna IP dapat berubah-ubah, akan tetapi mac address akan tetap, sehingga pengguna dapat di blok. Pada bagian ini, dibagian ***advanced,*** **src.MAC address** diisi dengan mac address yang ingin diblock, Seperti terlihat pada gambar dibawah ini:



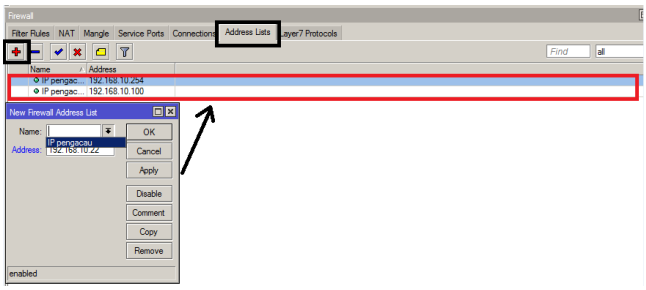
Untuk action, tetap pilih **drop**

Pada konfigurasi firewall mikrotik ada beberapa pilihan Action, diantaranya :

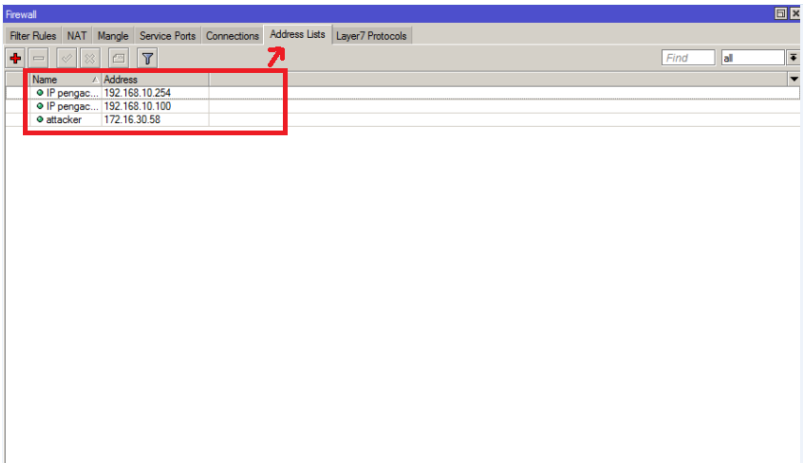
Accept : paket diterima dan tidak melanjutkan membaca baris berikutnya
Drop : menolak paket secara diam-diam (tidak mengirimkan pesan penolakan ICMP)
Reject : menolak paket dan mengirimkan pesan penolakan ICMP
Jump : melompat ke chain lain yang ditentukan oleh nilai parameter jump-target
Tarpit : menolak, tetapi tetap menjaga TCP connection yang masuk (membalas dengan

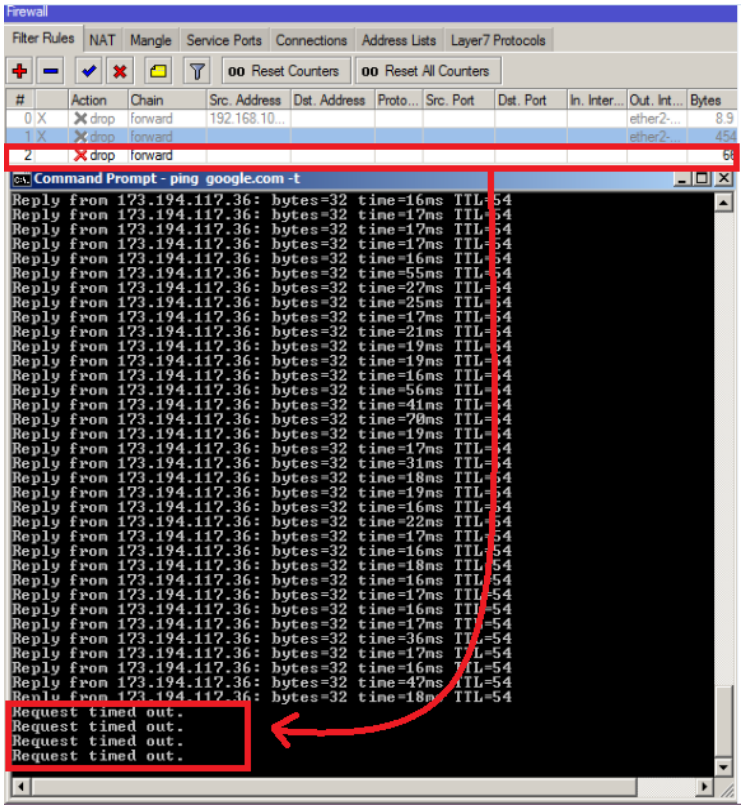
SYN/ACK untuk paket TCP SYN yang masuk)
Passthrough : mengabaikan rule ini dan menuju ke rule selanjutnya
log : menambahkan informasi paket data ke log

8. Apabila kita ingin mem-block beberapa IP, maka kita bisa mengelompokkan ip tersebut dalam suatu list.caranya : **IP->Firewall ,** Lalu pilih **Address list.** Pada bagian ini akan ditambah kan sebuah grup, dimisalkan diberi nama " IP Pengacau"

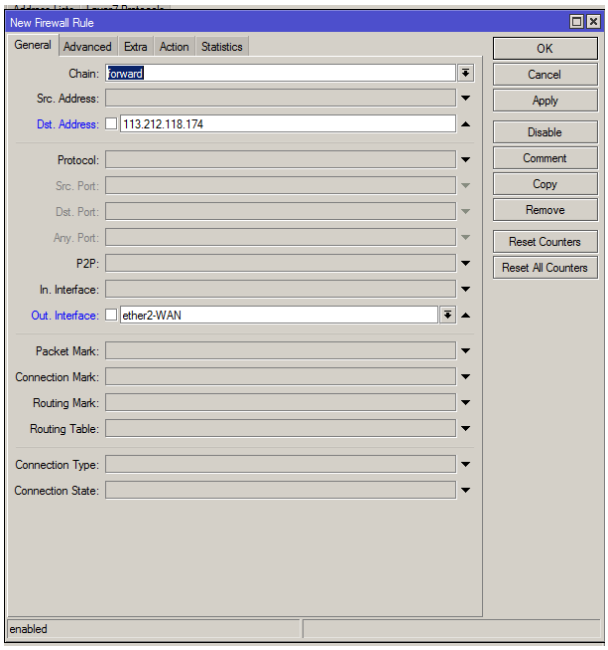


9. untuk menambahkan IP yang ingin dimasukkan ke list " IPpengacau" , dapat ditambahkan pada bagian **Source address list** dari menu *advanced*.



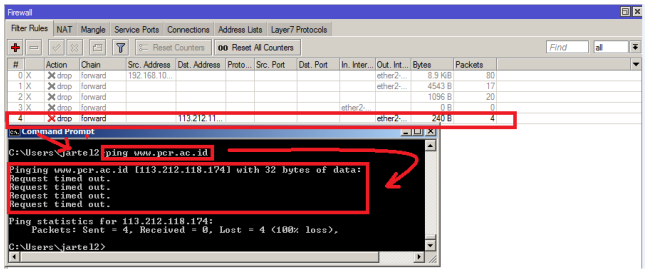


10. Selanjutnya, dari menu firewall yang ada pada mikrotik ini, kita juga dapat memblock situs atau IP tujuan yang kita anggap sebagi situs yang tidak baik.
klik **Filter Rules** lalu isi pada bagian **Dst.Adresses** (IP tujuan yang akan diblock). Dan untuk actionnya pilih **Drop.**

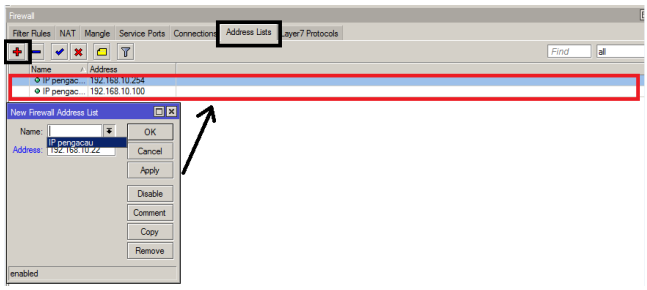


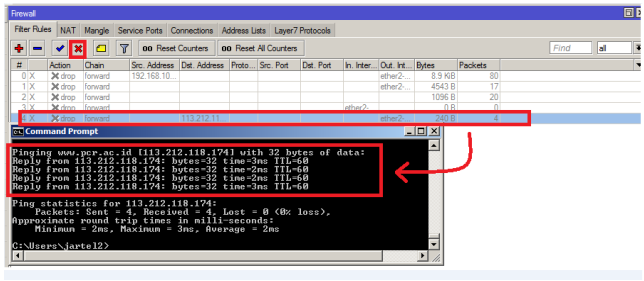
Disini kami mencoba memblock situs atau IP dari kampus Politeknik Caltex Riau.

Lalu kembali kita tes dengan melakukan PING ke IP situs Politeknik Caltex Riau



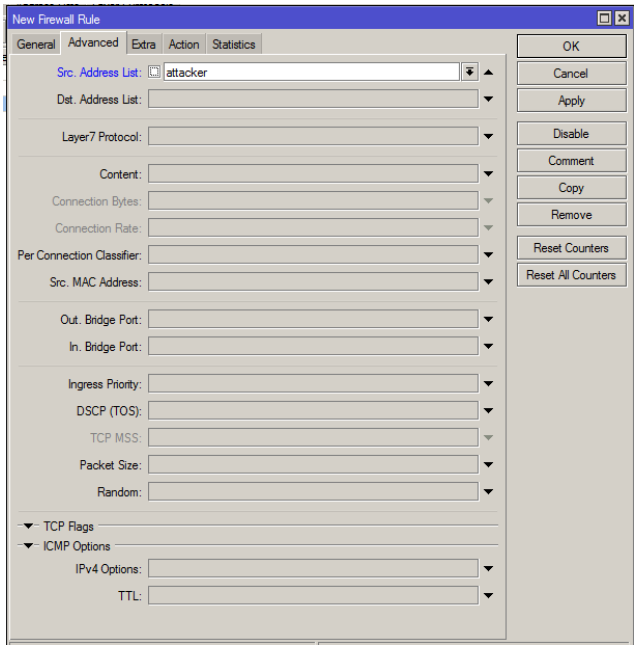
Dan jika ingin mengahpus block atau membatalkan block, dapat memberikan tanda silang pada konfigurasi tadi.





11. Selanjutnya, kita juga dapat memblock jaringan yang berasal dari luar, misalkan jaringan ini dicurigai sebagai aktifitas hacker.
Caranya kita tambahkan IP jaringan yang berasal dari luar mikrotik. Lalu untuk actionnya dipilih **Drop.**

Disini kami menamai "attacker"


New Firewall Rule
General
Advanced
Extra
Action
Statistics
Src. Address List:
attacker
Dst. Address List:
Layer7 Protocol:
Content:
Connection Bytes:
Connection Rate:
Per Connection Classifier:
Src. MAC Address:
Out. Bridge Port:
In. Bridge Port:
Ingress Priority:
DSCP (TOS):
TCP MSS:
Packet Size:
Random:
TCP Flags
ICMP Options
IPv4 Options:
TTL:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters