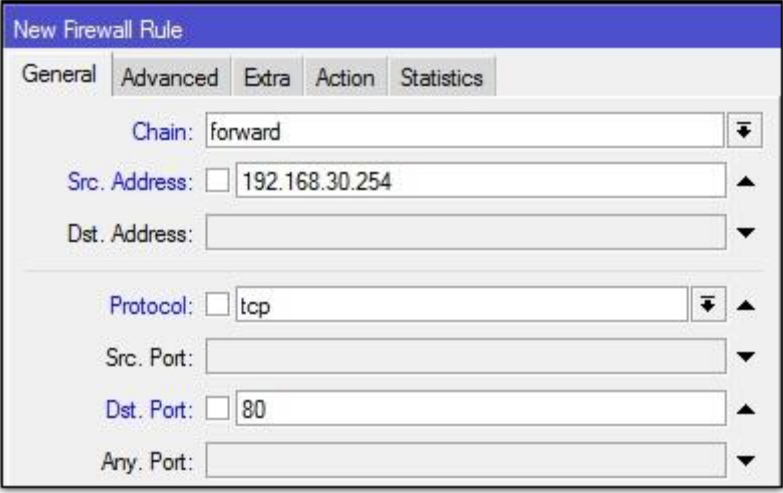


## Implementasi Firewall Filter

Secara umum, firewall filtering biasanya dilakukan dengan cara mendefinisikan IP address, baik itu src-address maupun dst-address. Misalnya Anda ingin blok komputer client yang memiliki ip tertentu atau ketika melakukan blok terhadap web tertentu berdasarkan ip web tersebut. Firewall tidak hanya digunakan untuk melakukan blok client agar tidak dapat mengakses resource tertentu, namun juga digunakan untuk melindungi jaringan local dari ancaman luar, misalnya virus atau serangan hacker. Biasanya serangan dari internet ini dilakukan dari banyak IP sehingga akan sulit bagi kita untuk melakukan perlindungan hanya dengan berdasarkan IP. Nah, sebenarnya ada banyak cara filtering selain berdasar IP Address, misalnya berdasar protocol dan port. Berikut contoh implementasi dengan memanfaatkan beberapa parameter di fitur firewall filter.

### Protokol dan Port

Penggunaan port dan protocol ini biasa di kombinasikan dengan IP address. Misalkan Anda ingin client tidak bisa browsing, namun masih bisa FTP, maka Anda bisa buat rule firewall yang melakukan blok di protocol TCP port 80. Ketika Anda klik tanda drop down pada bagian protocol, maka akan muncul opsi protocol apa saja yang akan kita filter. Parameter ini akan kita butuhkan ketika kita ingin melakukan blok terhadap aplikasi dimana aplikasi tersebut menggunakan protocol dan port yang spesifik.



The screenshot shows the 'New Firewall Rule' dialog box with the following configuration:

- Chain:** forward
- Src. Address:** 192.168.30.254
- Dst. Address:** (empty)
- Protocol:** tcp
- Src. Port:** (empty)
- Dst. Port:** 80
- Any. Port:** (empty)

### Interface

Interface secara garis besar ada 2, input interface dan output interface. Cara menentukannya adalah dengan memperhatikan dari interface mana traffick tersebut masuk ke router, dan dari interface mana traffick tersebut keluar meninggalkan router. Misalkan Anda terkoneksi ke internet melalui router mikrotik, kemudian Anda ping ke [www.mikrotik.co.id](http://www.mikrotik.co.id) dari laptop Anda, maka input interface adalah interface yang terkoneksi ke laptop Anda, dan output interface adalah interface yang terkoneksi ke internet. Contoh penerapannya adalah ketika Anda ingin menjaga keamanan router, Anda tidak ingin router bisa diakses dari internet. Dari kasus tersebut Anda bisa lakukan filter terhadap koneksi yang masuk ke router dengan mengarahkan opsi in-interface pada interface yang terkoneksi ke internet .

In. Interface:  ▼ ▲

Out. Interface:  ▼

### Parameter P2P

Sebenarnya ada cara yang cukup mudah dan simple untuk melakukan filtering terhadap traffick P2P seperti torrent atau edonkey. Jika sebelumnya Anda menggunakan banyak rule, Anda bisa sederhanakan dengan menentukan parameter P2P pada rule firewall filter. Jika Anda klik bagian drop down, akan muncul informasi program p2p yang dapat di filter oleh firewall.

P2P:  ▼ ▲

### Mangle

Kita biasanya membuat mangle untuk menandai paket/koneksi, kemudian kita gunakan untuk bandwidth management. Akan tetapi kita juga bisa membuat mangle untuk melakukan filtering. Firewall filter tidak dapat melakukan penandaan pada paket atau koneksi, akan tetapi kita bisa kombinasikan mangle dan firewall filter. Pertama, kita tandai terlebih dahulu paket atau koneksi dengan mangle, kemudian kita definisikan di firewall filter.

Packet Mark:  ▼ ▲

Connection Mark:  ▼

Routing Mark:  ▼

Routing Table:  ▼

### Connection State

Jika Anda tidak ingin ada paket - paket invalid lalu lalang di jaringan Anda, Anda juga bisa melakukan filtering dengan mendefinisikan parameter connection state. Paket invalid merupakan paket yang tidak memiliki koneksi dan tidak berguna sehingga hanya akan membebani resource jaringan. Kita bisa melakukan drop terhadap paket - paket ini dengan mendefinisikan parameter connection state.

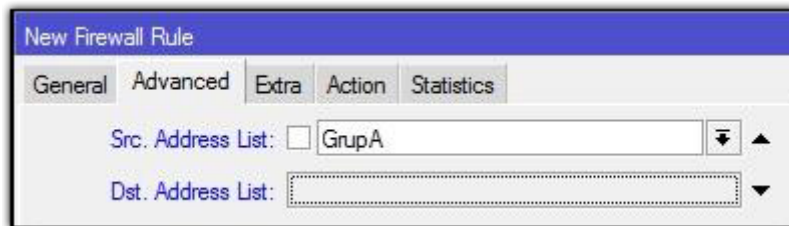
Connection Type:  ▼

Connection State:  ▼ ▲

### Address List

Ada saat dimana kita ingin melakukan filtering terhadap beberapa ip yang tidak berurutan atau acak.

Apabila kita buat rule satu per satu, tentu akan menjadi hal yang melelahkan. Dengan kondisi seperti ini, kita bisa menerapkan grouping IP membuat "address list". Pertama, buat daftar ip di address list, kemudian terapkan di filter rule Anda. Opsi untuk menambahkan parameter "Address List" di firewall ada di tab Advanced. Ada 2 tipe address list, "Src. Address List" dan "Dst. Address List. Src Address List adalah daftar sumber ip yang melakukan koneksi, Dst Address List adalah ip tujuan yang hendak diakses.



### Layer 7 Protocol

Jika Anda familiar dengan regexp, Anda juga bisa menerapkan filtering pada layer7 menggunakan firewall filter. Di mikrotik, penambahan regexp bisa dilakukan di menu Layer 7 Protocol. Setelah Anda menambahkan regexp, Anda bisa melakukan filtering dengan mendefinisikan Layer 7 Protocol pada rule filter yang Anda buat. Perlu diketahui bahwa penggunaan regexp, akan membutuhkan resource CPU yang lebih tinggi dari rule biasa.



### Content

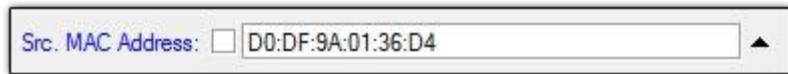
Saat kita hendak melakukan blok terhadap website, salah satu langkah yang cukup mudah untuk melakukan hal tersebut adalah dengan melakukan filter berdasarkan content. Content merupakan string yang tertampil di halaman website. Dengan begitu, website yang memiliki string yang kita isikan di content akan terfilter oleh firewall. Misalkan kita ingin block www.facebook.com maka cukup isi parameter content dengan string `facebook` dan action drop, maka website facebook baik HTTP maupun HTTPS tidak dapat diakses.



### Mac address

Ketika kita melakukan filter by ip address, terkadang ada user yang nakal dengan mengganti ip address. Untuk mengatasi kenakalan ini, kita bisa menerapkan filtering by mac-address. Kita catat informasi mac address yang digunakan user tersebut, kemudian kita tambahkan parameter Src. Mac Address di rule

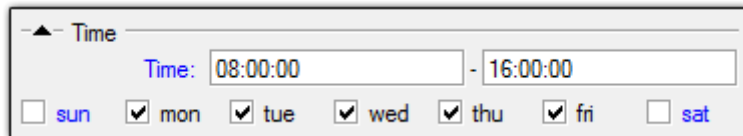
firewall kita. Dengan begitu selama user tersebut masih menggunakan device yang sama, dia tetap ter-filter walaupun berganti ip.



A screenshot of a configuration window showing a text field for "Src. MAC Address:". The field contains the value "D0:DF:9A:01:36:D4". There is a small upward-pointing arrow icon to the right of the text field.

### Time

Salah satu solusi alternatif selain kita harus repot membuat scheduler dan script, kita bisa memanfaatkan fitur time di firewall filter. Fitur ini akan menentukan kapan rule firewall tersebut dijalankan. Bukan hanya untuk menentukan jam saja, fitur ini juga bisa digunakan untuk menentukan hari apa saja rule tersebut berjalan. Misalkan kita ingin melakukan block facebook di jam kerja, maka kita bisa buat rule firewall yang melakukan block facebook yang dijalankan dari jam 08:00 sampai jam 16:00 selain hari Sabtu dan Minggu. Sebelum anda membuat rule firewall dengan parameter **time**, pastikan Anda sudah set NTP di router Anda agar waktu router sesuai dengan waktu real.



A screenshot of a configuration window titled "Time". It shows a time range from "08:00:00" to "16:00:00". Below the time range, there are checkboxes for the days of the week: "sun" (unchecked), "mon" (checked), "tue" (checked), "wed" (checked), "thu" (checked), "fri" (checked), and "sat" (unchecked).

Saat Anda membuat rule firewall, usahakan untuk membuat rule yang spesifik. Semakin spesifik rule yang kita buat, maka semakin optimal pula rule tersebut akan berjalan.