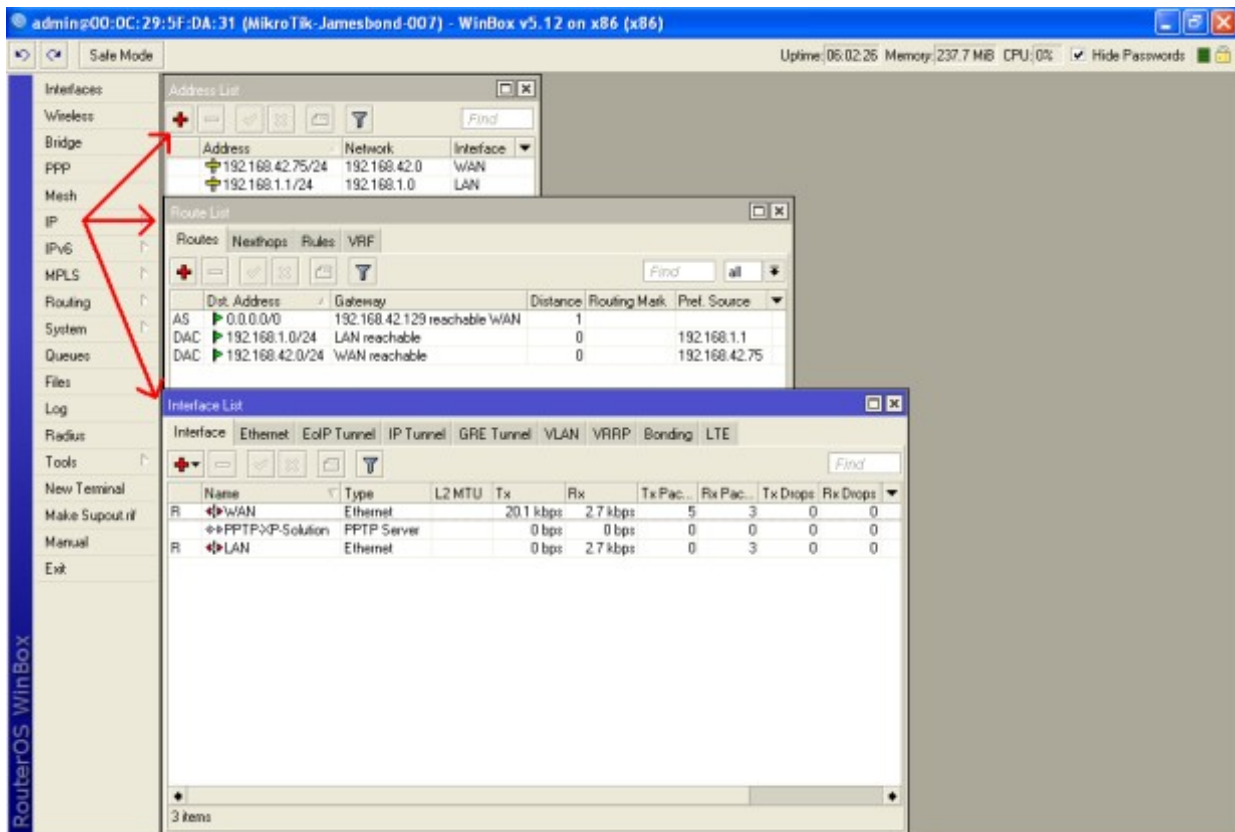


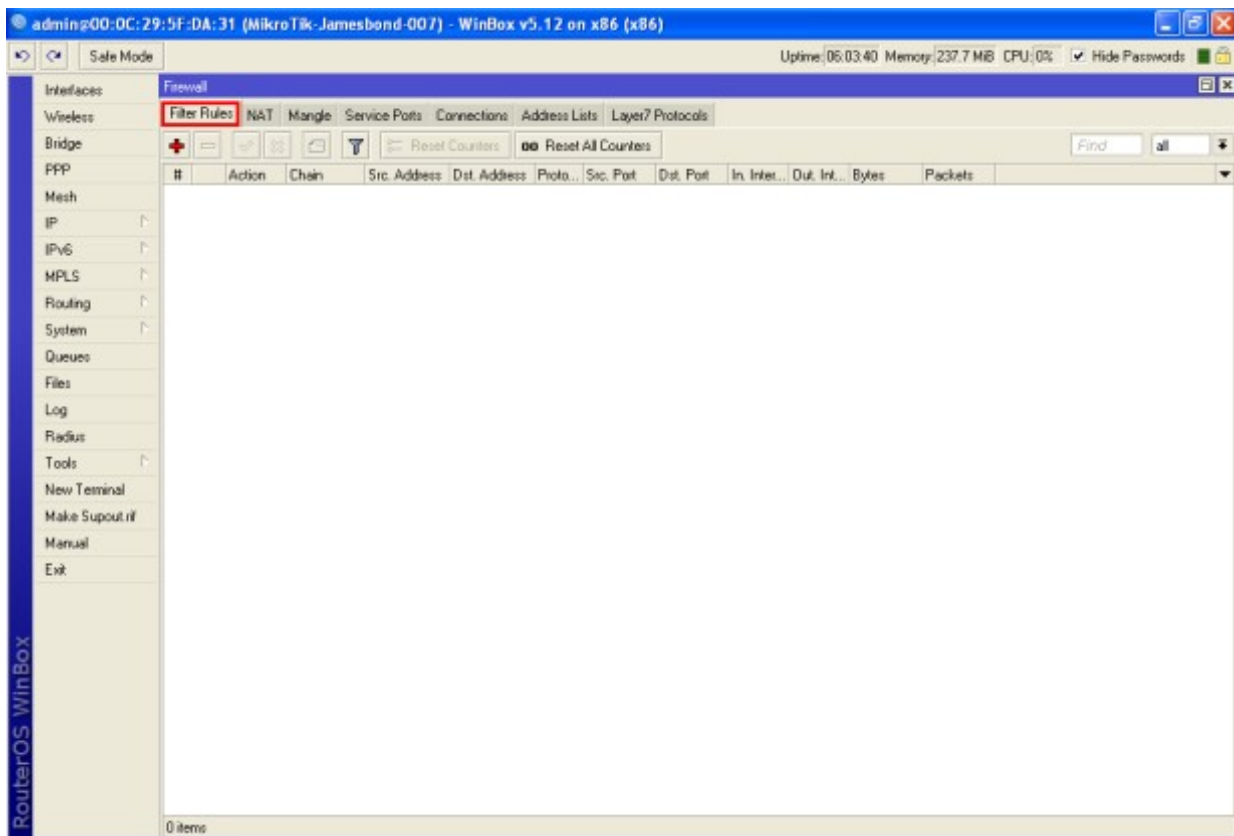
Firewall

LAB-2

Berikut ini adalah **Step by Step Konfigurasi Mikrotik Firewall** dalam bahasa yang simple dan mudah di pahami secara awam. Misalnya pada Mikrotik ini dengan Interface bernama **LAN** dan **WAN**. Contoh IP Address WAN adalah **192.168.42.75** dan IP Address LAN adalah **192.168.1.1**. Lebih detailnya dapat kita lihat pada gambar dibawah ini :

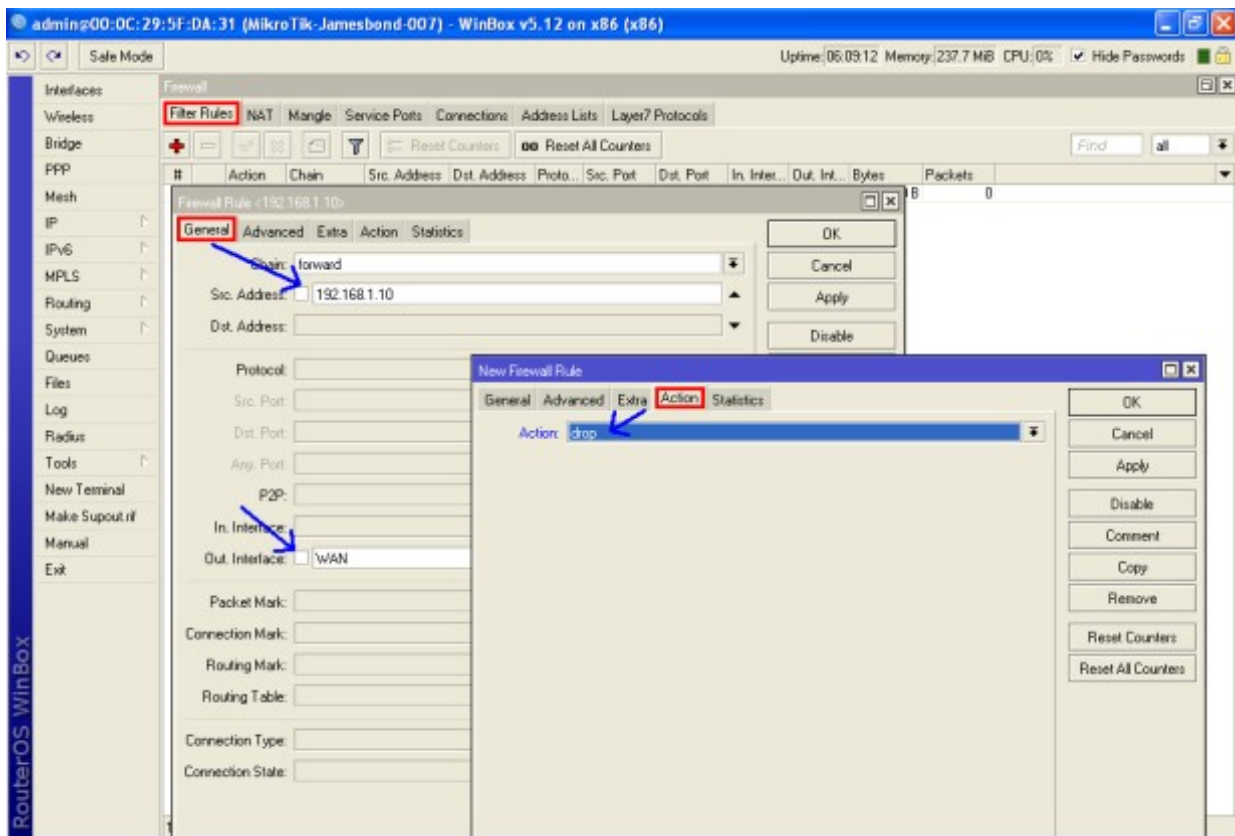


Untuk memulai konfigurasi Firewall, kita pilih menu : **IP --> FIREWALL**. Selanjutnya kita dapat menambahkan pengaturan **Firewall** secara **Logika**.

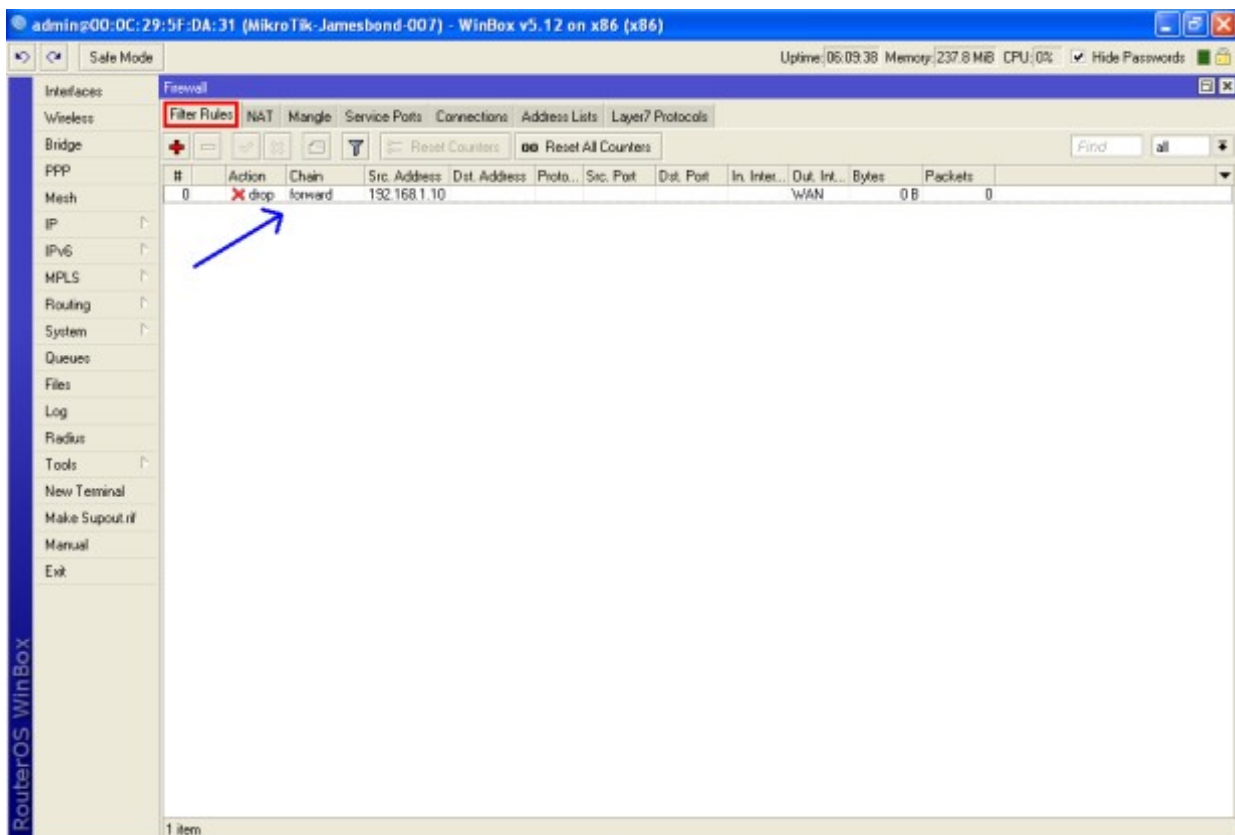


1. MEMBUAT FIREWALL UNTUK MEMBLOCK AKSES INTERNET DARI 1 IP ADDRESS CLIENT.

- Buat **New Firewall Rules**, pada Option “**GENERAL**”, pilih Chain : “**FORWARD**”.
- Lalu kita pilih / isi **Source Address** dengan IP Address dari Client yang akan kita Block. Misalnya Client dengan IP : **192.168.1.10**.
- Out Interface** kita isi dengan interface : **WAN**.
- Selanjutnya pada Option “**ACTION**”, kita pilih : “**DROP**”.
- Jadi Firewall ini berarti : “Jika ada Client dengan IP : **192.168.1.10** yang akan mengakses internet dengan **OUTGOING** melalui Interface **WAN**, maka koneksi ini akan di **DROP** oleh Mikrotik.



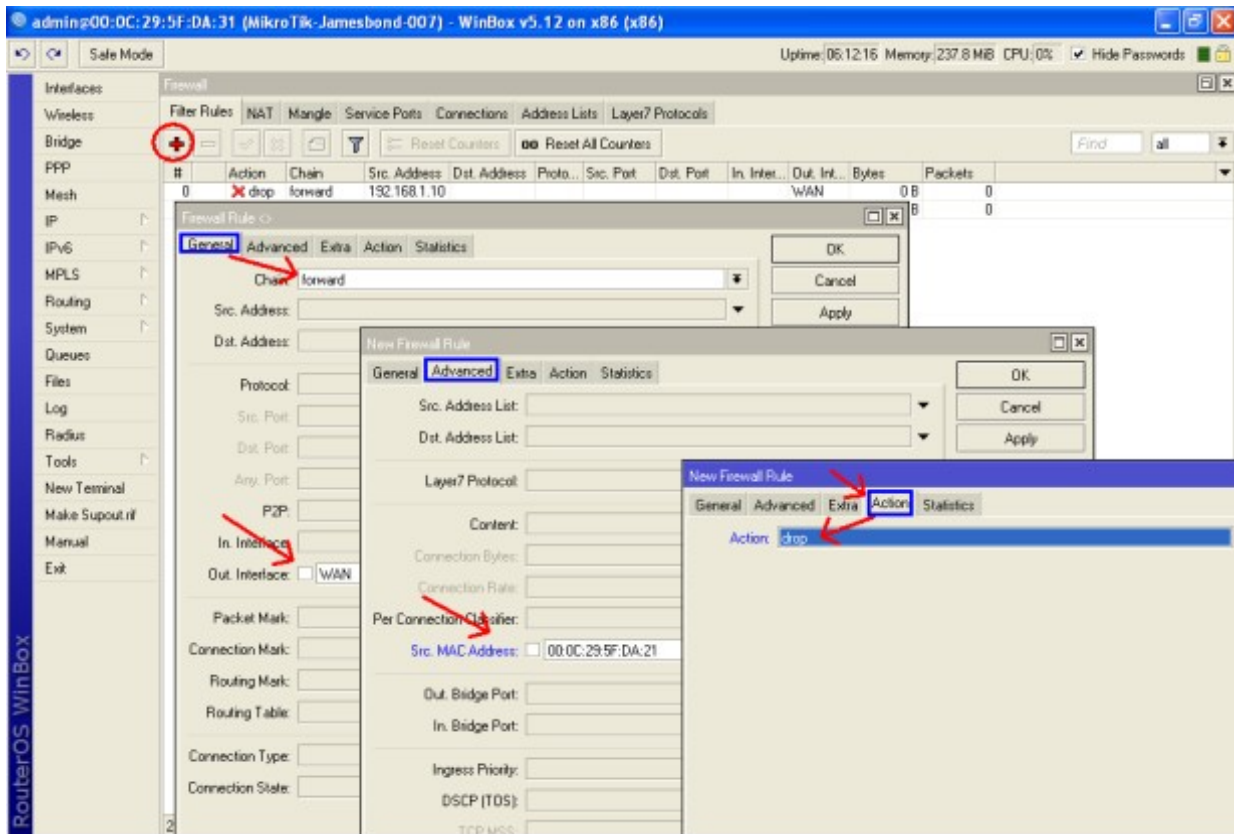
•Dibawah ini tampilan Firewall Rule yang barusan kita buat.



2. MEMBUAT FIREWALL UNTUK MEMBLOCK AKSES INTERNET DARI 1 MAC ADDRESS CLIENT.

•Buat **New Firewall Rules**, pada Option “**GENERAL**”, pilih Chain : “**FORWARD**”.

- **Out Interface** kita isi dengan interface : **WAN**.
- Selanjutnya pada menu “**ADVANCED**”, isikan pada menu “**Source Mac Address**” daripada Mac Address yang dimiliki oleh Client yang akan kita Blokir akses internetnya.
- Selanjutnya pada Option “**ACTION**”, kita pilih : “**DROP**”.
- Jadi Firewall ini berarti : “Jika ada Client dengan **Mac Address** sesuai Mac target yang akan mengakses internet dengan **OUTGOING** melalui Interface **WAN**, maka koneksi ini akan di **DROP** oleh Mikrotik.



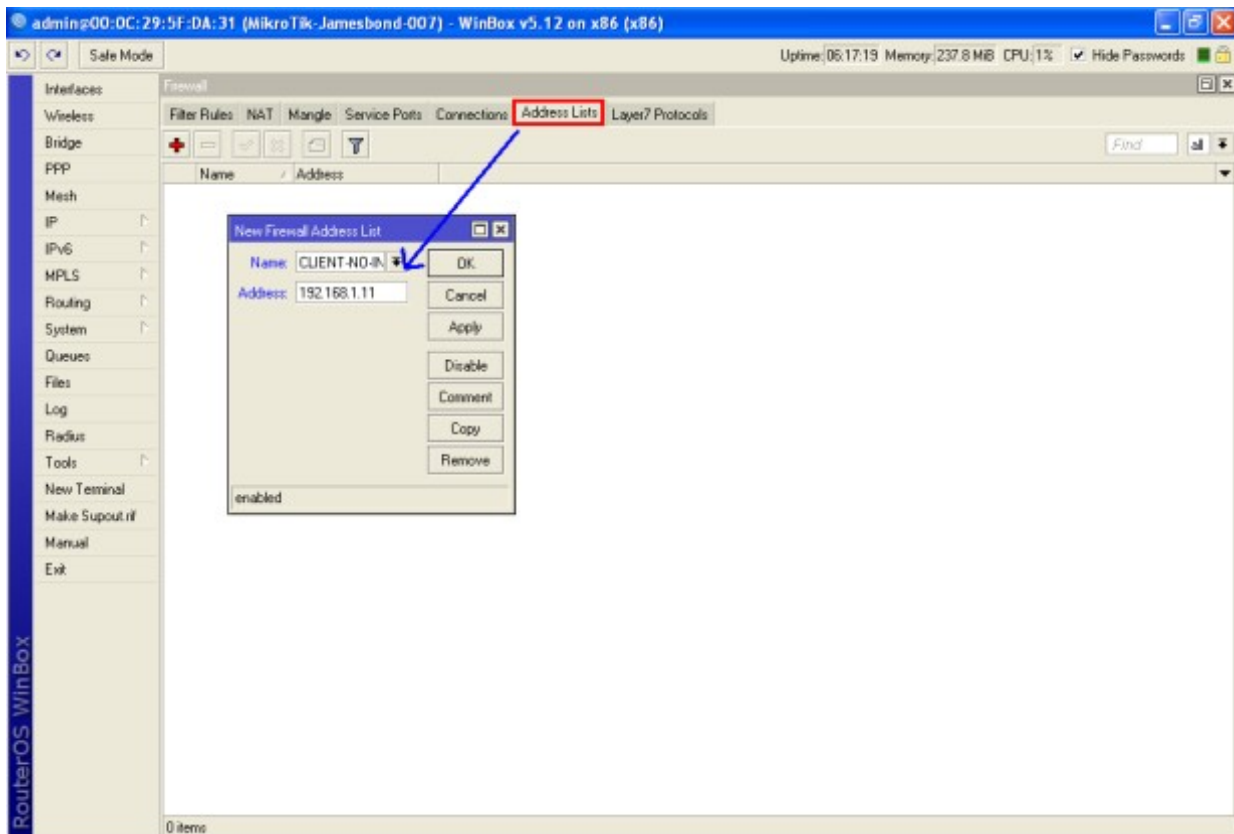
3. MEMBUAT FIREWALL UNTUK MEMBLOCK AKSES INTERNET DARI SEKELOMPOK IP ADDRESS CLIENT.

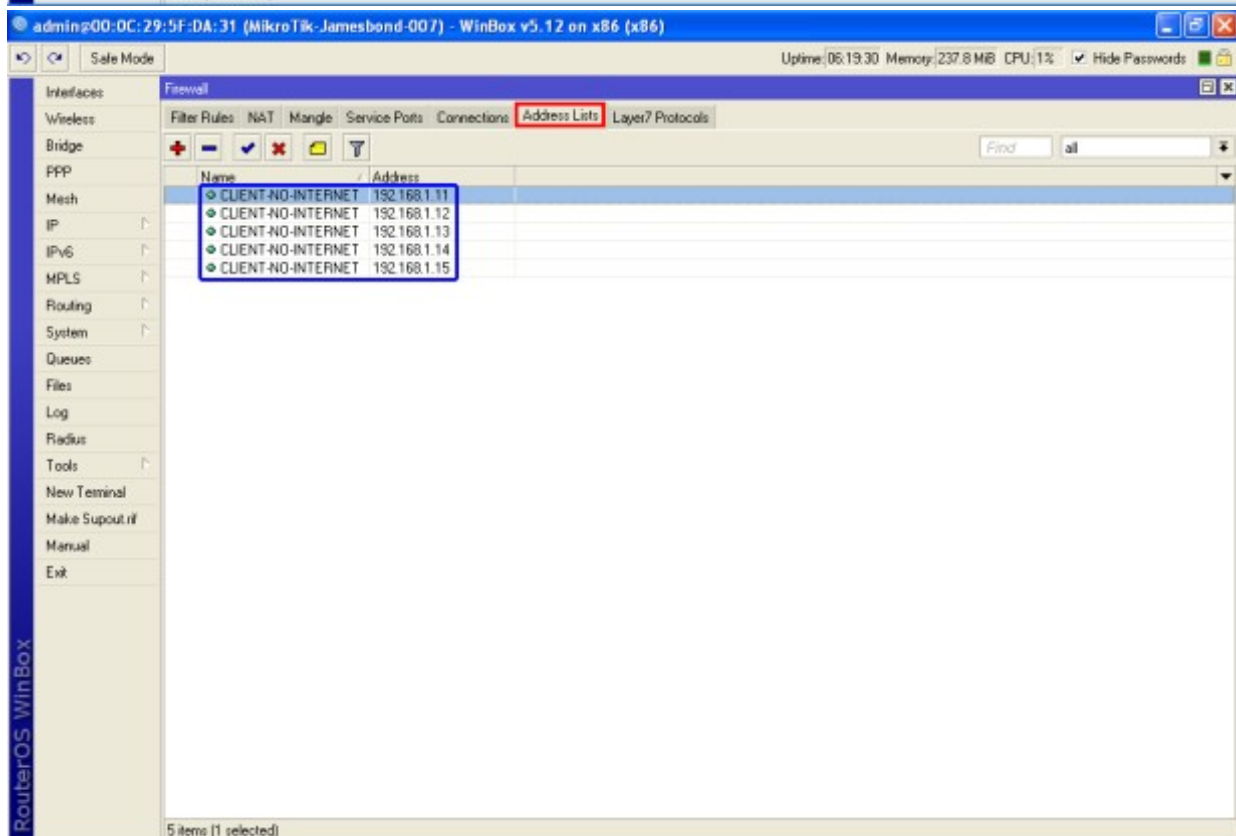
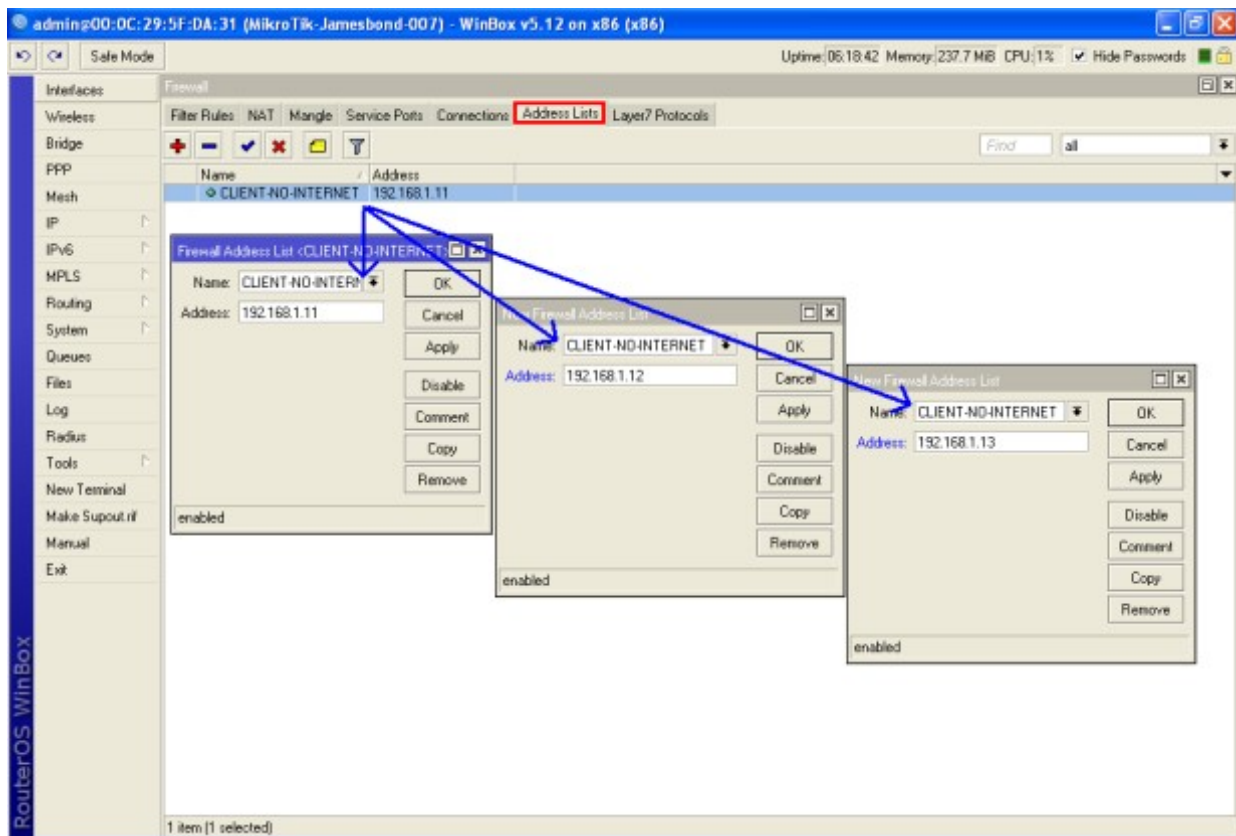
- Pertama kita buat lebih dulu sejumlah IP Address pada menu **Firewall** -> **Address List**. Misalnya kita berikan nama “**CLIENT NO INTERNET**”.
- Buatlah sejumlah daftar IP Address Client dari LAN kita yang akan di block akses internet-nya.
- Selanjutnya kita buat sebuah **New Firewall Rules**, pada Option “**GENERAL**”, pilih Chain : “**FORWARD**”.
- Out Interface** kita isi dengan interface : **WAN**.

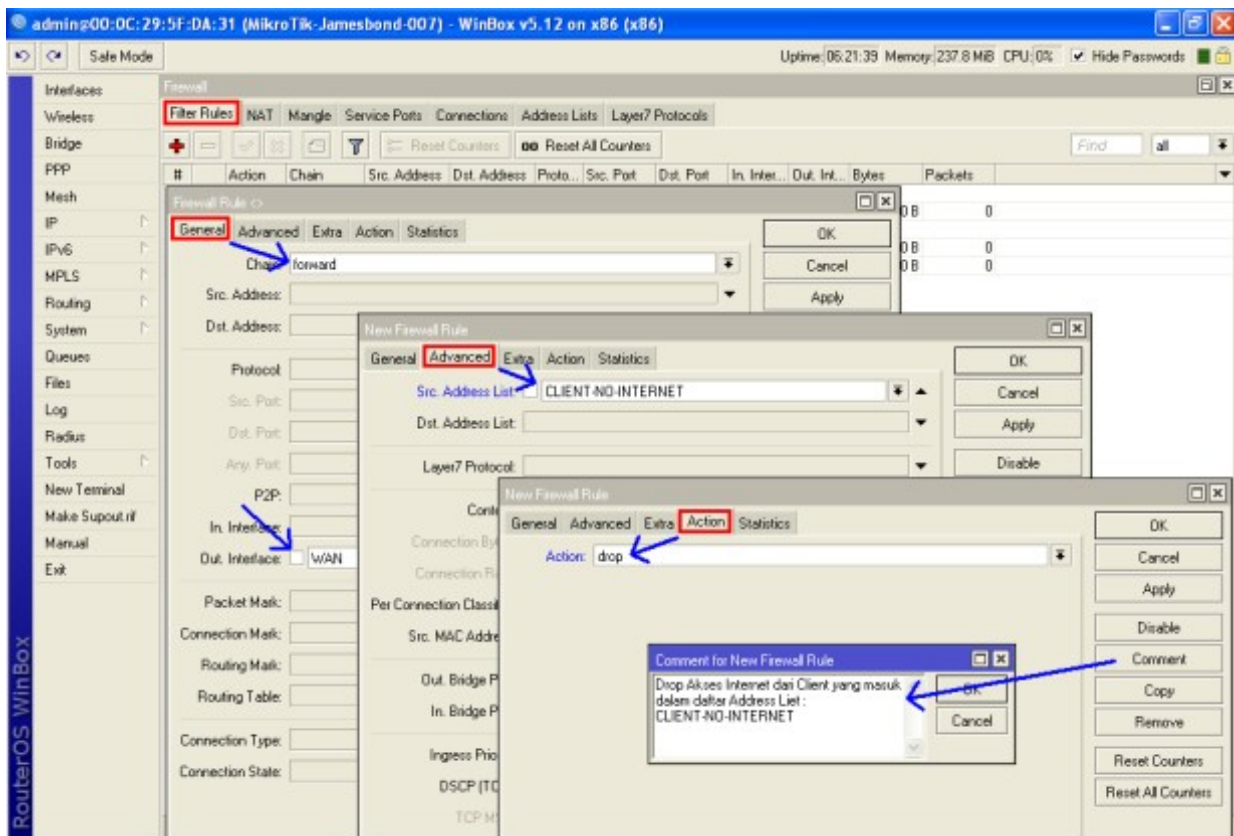
- Selanjutnya pada menu“**ADVANCED**”, isikan pada menu “**Source Address List**” daripada Daftar Address List yang telah kita buat untuk memblokir akses internetnya. Kita pilih nama : “**CLIENT NO INTERNET**”.

- Selanjutnya pada Option “**ACTION**”, kita pilih : “**DROP**”.

- Jadi Firewall ini berarti : “Jika ada Client dengan **IP Address** yang terdaftar pada “**CLIENT NO INTERNET**” yang akan mengakses internet dengan **OUTGOING** melalui Interface **WAN**, maka koneksi ini akan di **DROP** oleh Mikrotik.

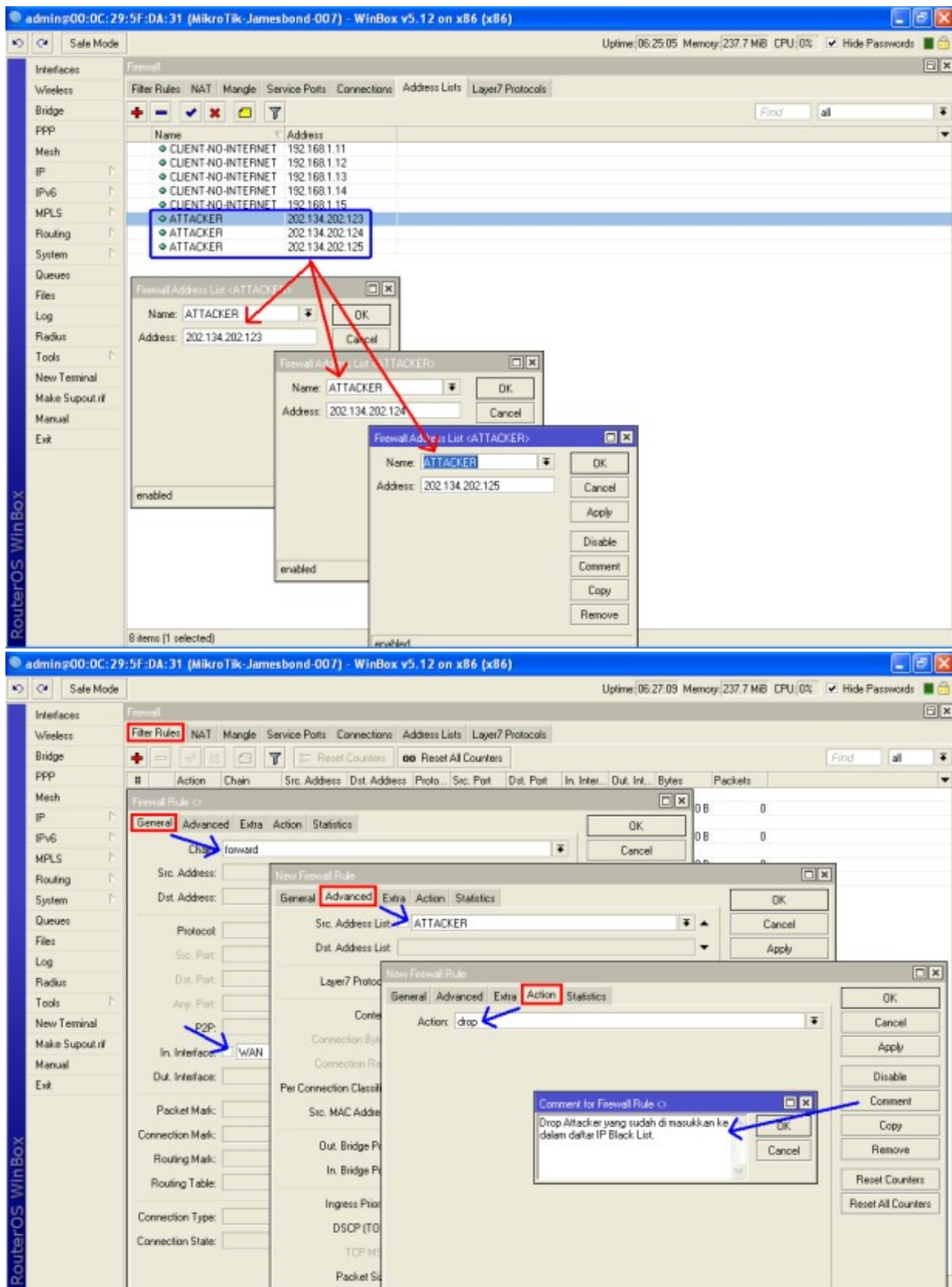






4. MEMBUAT FIREWALL UNTUK MEMBLOCK AKSES INTERNET DARI SEKELOMPOK IP ADDRESS ATTACKER.

- Pertama kita buat lebih dulu sejumlah IP Address pada menu **Firewall** -> **Address List**. Misalnya kita berikan nama "**ATTACKER**".
- Buatlah sejumlah daftar IP Address dari IP yang kita identifikasikan sebagai Black List IP Address dan kita akan di block akses internet-nya. IP Address ini biasanya terdeteksi sebagai **LOG MERAH** atau **Illegal Access** pada Mikrotik kita.
- Selanjutnya kita buat sebuah **New Firewall Rules**, pada Option "**GENERAL**", pilih Chain : "**FORWARD**".
- In **Interface** kita isi dengan interface : **WAN**.
- Selanjutnya pada menu "**ADVANCED**", isikan pada menu "**Source Address List**" daripada Daftar Address List yang telah kita buat untuk memblokir akses internetnya. Kita pilih nama : "**ATTACKER**".
- Selanjutnya pada Option "**ACTION**", kita pilih : "**DROP**".
- Jadi Firewall ini berarti : "Jika ada orang atau system dengan **IP Address** yang terdaftar pada "**ATTACKER**" yang akan mengakses IP Public / IP WAN kita yang masuk melalui Interface **WAN**, maka koneksi ini akan di **DROP** oleh Mikrotik.



5. MEMBUAT FIREWALL UNTUK MEMBLOCK AKSES INTERNET DARI CLIENT KE SUATU WEBSITES TERLARANG.

- Buat **New Firewall Rules**, pada Option "**GENERAL**", pilih Chain : "**FORWARD**".

- Lalu kita pilih / isi **Destination Address** dengan IP Address dari websites yang akan kita Block. Misalnya Websites **http://www.porno.com** dengan IP Public : **208.87.35.103**.

- Out Interface** kita isi dengan interface : **WAN**.

- Selanjutnya pada Option “**ACTION**”, kita pilih : “**DROP**”.

- Jadi Firewall ini berarti : “Jika ada Client dari jaringan LAN kita yang akan mengakses Websites <http://www.porno.com> dengan IP Public : **208.87.35.103** dengan **OUTGOING** melalui Interface **WAN**, maka koneksi ini akan di **DROP** oleh Mikrotik.

