8 Modul

Firewall

TUJUAN

1. Mahasiswa memahami cara kerja firewall
2. Mahasiswa dapat melakukan konfigurasi firewall pada router MikroTik

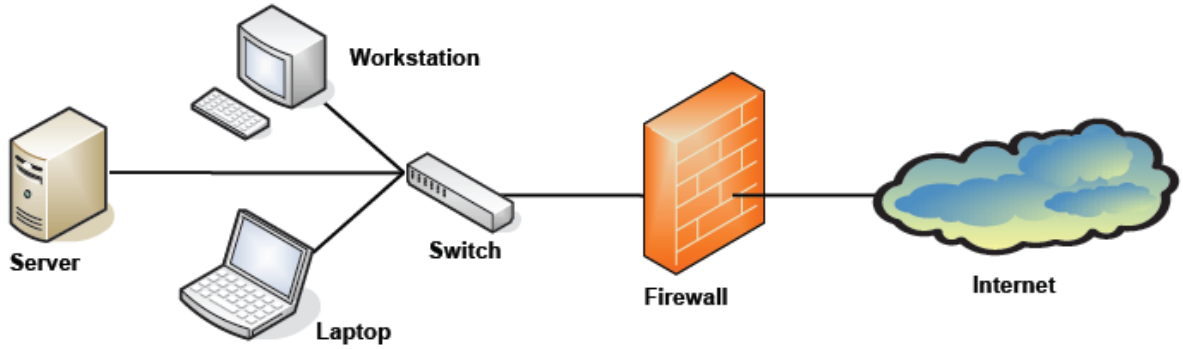
Alat	Aplikasi
Labtop	GNS3
MikroTik	Winbox

Kata Kunci

Teori

Apa itu Firewall?

Firewall adalah perangkat yang berfungsi untuk memeriksa dan menentukan paket data yang dapat keluar atau masuk dari sebuah jaringan.

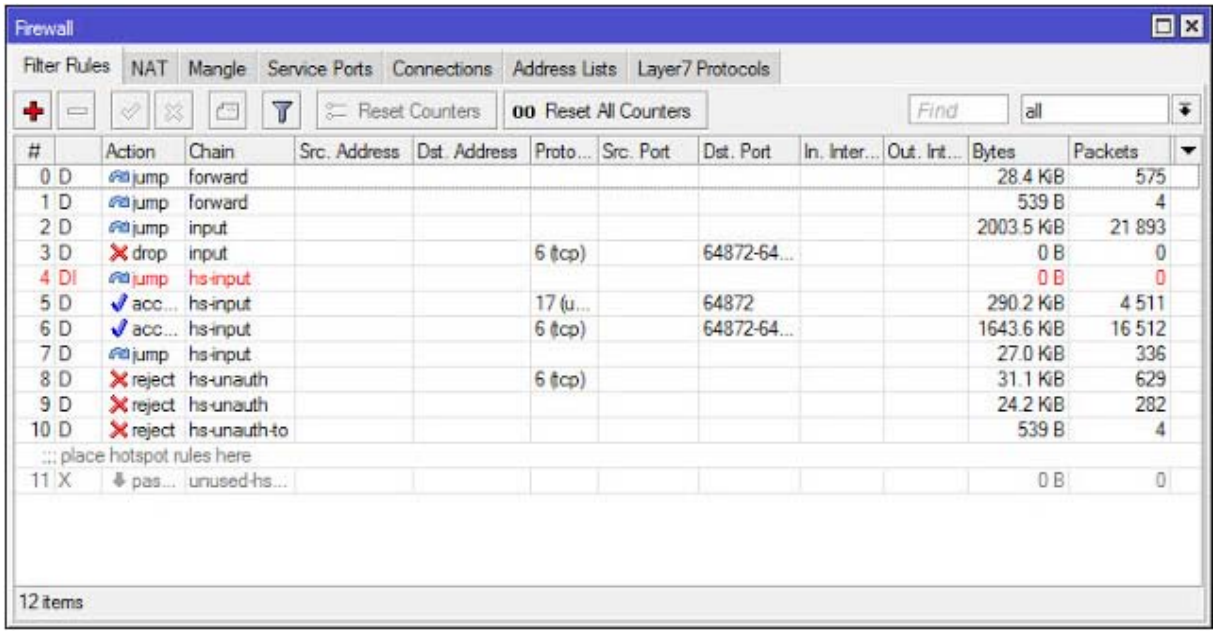


MikroTik RouterOS memiliki implementasi firewall yang sangat kuat dengan fitur termasuk:

- stateful packet inspection
- Layer-7 protocol detection
- peer-to-peer protocols filtering

- traffic classification by:
- source MAC address
- IP addresses (network or list) and address types (broadcast, local, multicast, unicast)
- port or port range
- IP protocols
- protocol options (ICMP type and code fields, TCP flags, IP options and MSS)
- interface the packet arrived from or left through
- internal flow and connection marks
- DSCP byte
- packet content
- rate at which packets arrive and sequence numbers
- packet size
- packet arrival time

Mengakses **Firewall Mikrotik** via **Winbox** melalui menu **IP → Firewall**



Firewall beroperasi dengan menggunakan aturan firewall. Setiap aturan terdiri dari dua bagian :

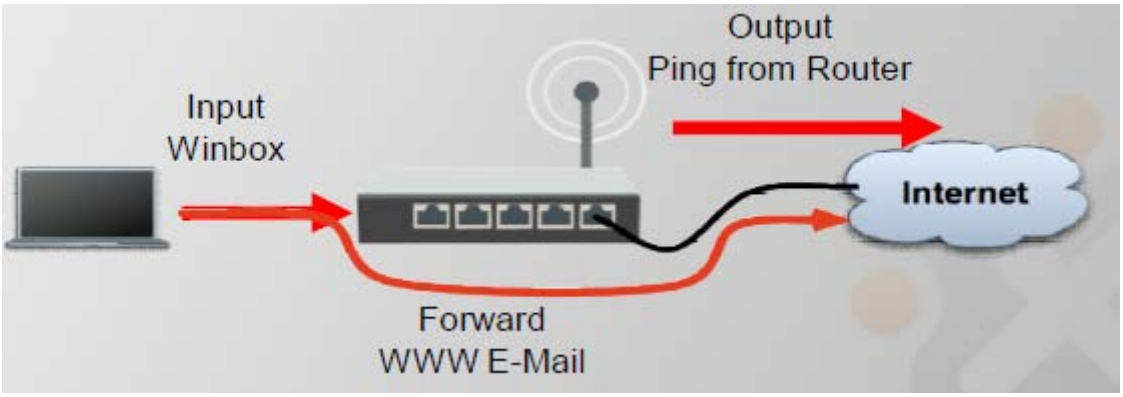
- Matcher yang sesuai arus lalu lintas terhadap kondisi yang diberikan
- Tindakan yang mendefinisikan apa yang harus dilakukan dengan paket yang cocok

Ada **3 chain** yang telah ditetapkan pada RouterOS Mikrotik :

- **Input** : digunakan untuk memproses paket memasuki router melalui salah satu interface dengan alamat IP tujuan yang merupakan salah satu alamat router. Chain input berguna untuk membatasi akses konfigurasi terhadap Router Mikrotik.
- **Forward** : digunakan untuk proses paket data yang melewati router.

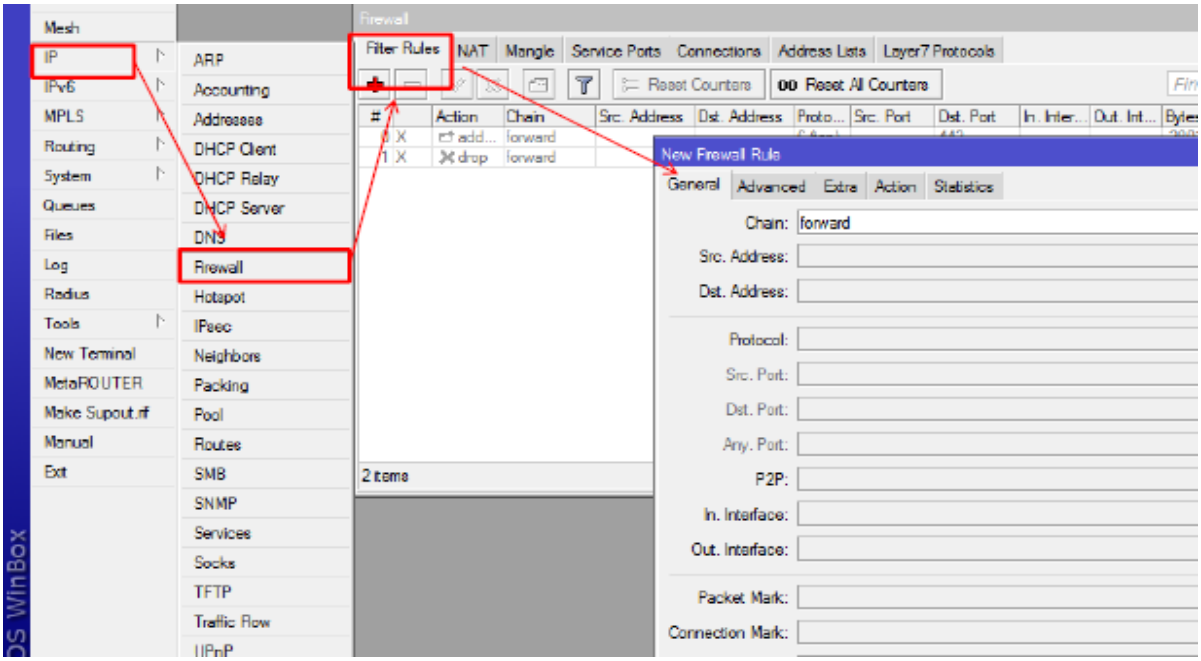
- **Output** : digunakan untuk proses paket data yang berasal dari router dan meninggalkan melalui salah satu interface.

Packet Flow



Firewall Filter Rule

- Prinsip IF….THEN….
- IF (jika) packet memenuhi syarat kriteria yang kita buat.
- THEN (maka) action apa yang akan dilakukan pada packet tersebut



Connection State

Connection State (Status paket data yang melalui router)

- **Invalid** : paket tidak dimiliki oleh koneksi apapun, tidak berguna.
- **New** : paket yang merupakan pembuka sebuah koneksi/paket pertama dari sebuah koneksi.
- **Established** : merupakan paket kelanjutan dari paket dengan status new.
- **Related** : paket pembuka sebuah koneksi baru, tetapi masih berhubungan denga koneksi sebelumnya.

Action Filter Firewall RouterOS Mikrotik

Pada konfigurasi firewall mikrotik ada beberapa pilihan Action, diantaranya :

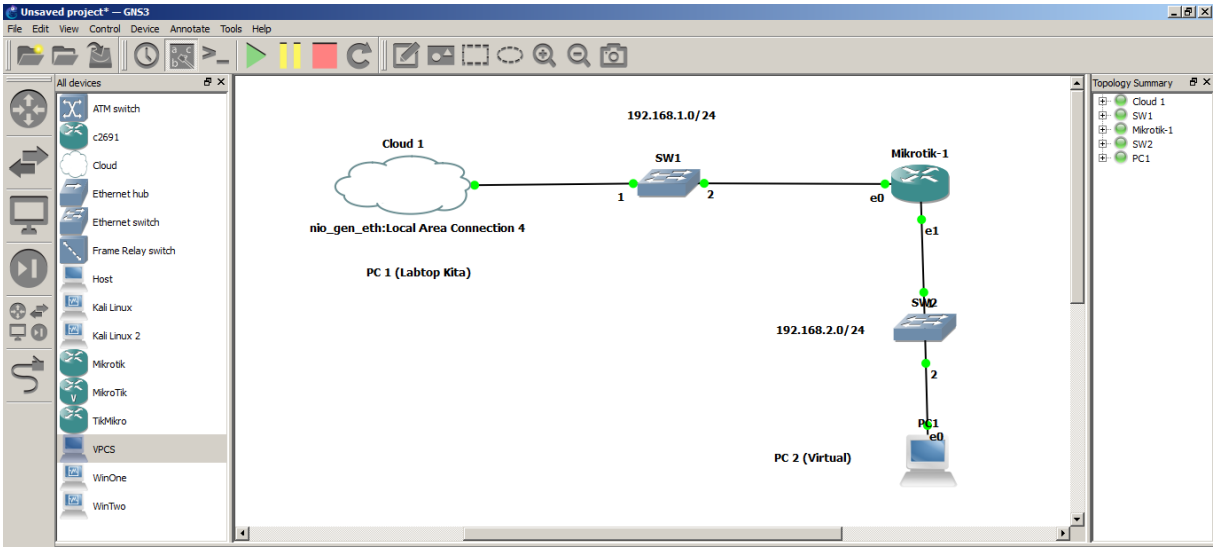
- **Accept** : paket diterima dan tidak melanjutkan membaca baris berikutnya
- **Drop** : menolak paket secara diam-diam (tidak mengirimkan pesan penolakan ICMP)
- **Reject** : menolak paket dan mengirimkan pesan penolakan ICMP
- **Jump** : melompat ke chain lain yang ditentukan oleh nilai parameter 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

Lab

Melindungi Router dengan Filter Rule

Dalam pengaplikasiannya, terkadang kita was-was terhadap router mikrotik kita, kita takut mikrotik kita bisa ada yang hack, pasti kita butuh untuk melindungi router kita sendiri. Dalam hal ini, kita akan menggunakan konsep Accep few and Drop Any, yang artinya Terima beberapa dan Tolak Semua. Bagaimana caranya ? langsung aja:

Buatlah desain topologi seperti gambar di bawah ini menggunakan GNS3.



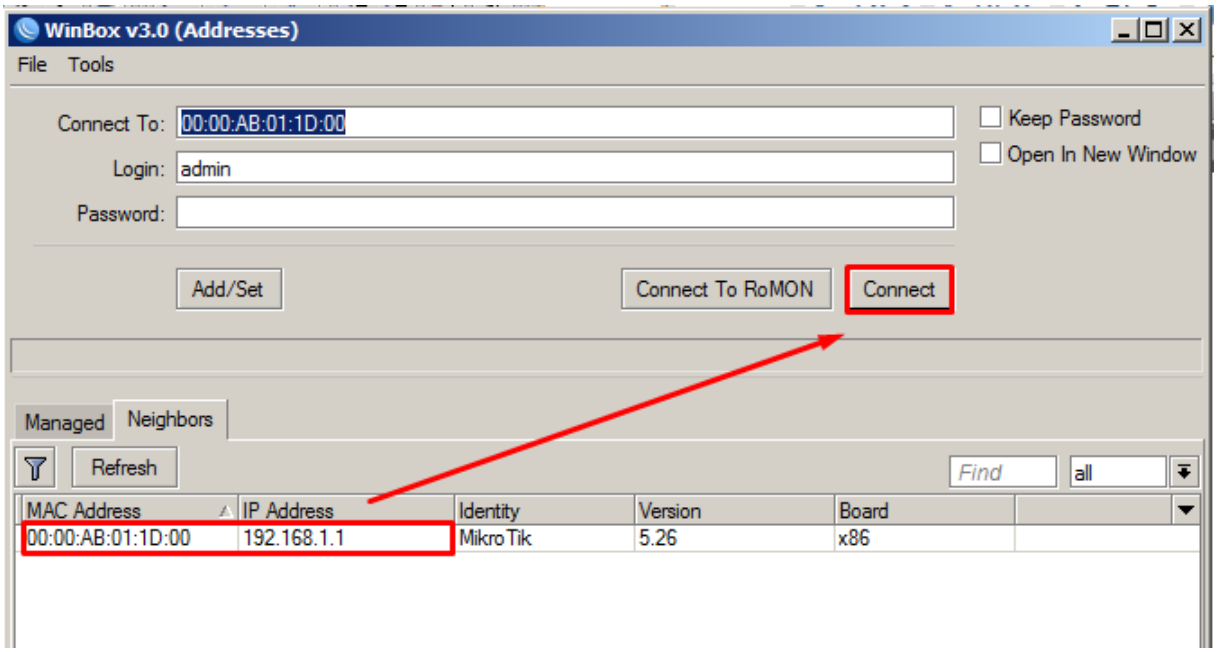
Jalankan GNS3 →**Run**

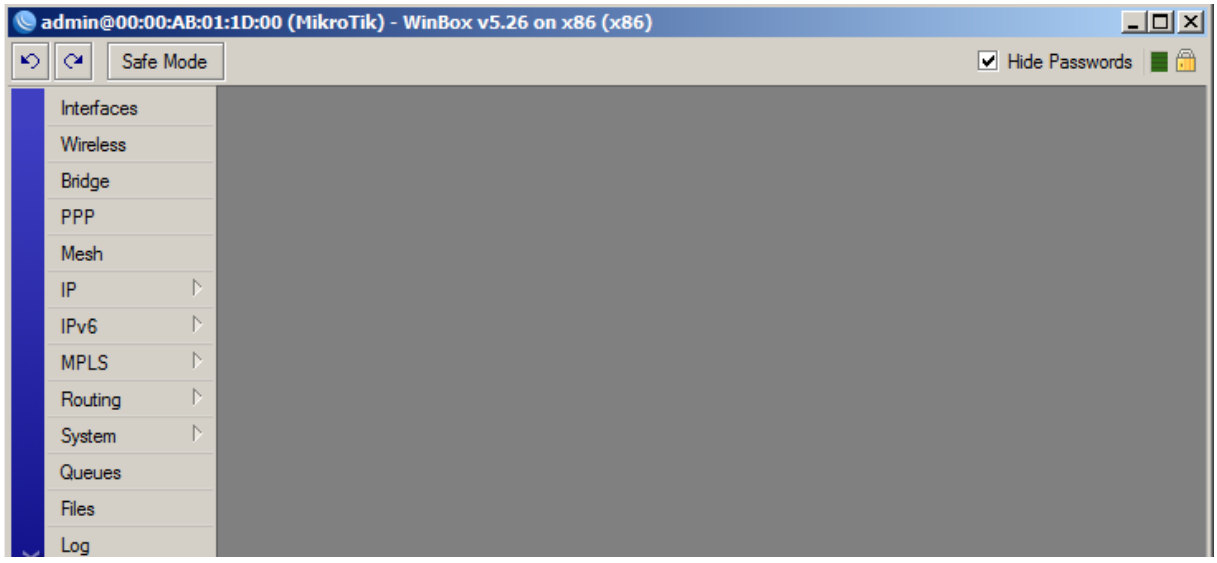
Masuk ke Router melalui **Console** dan isikan **IP address** sesuai dengan **interface** masing-masing.

Sintaks =

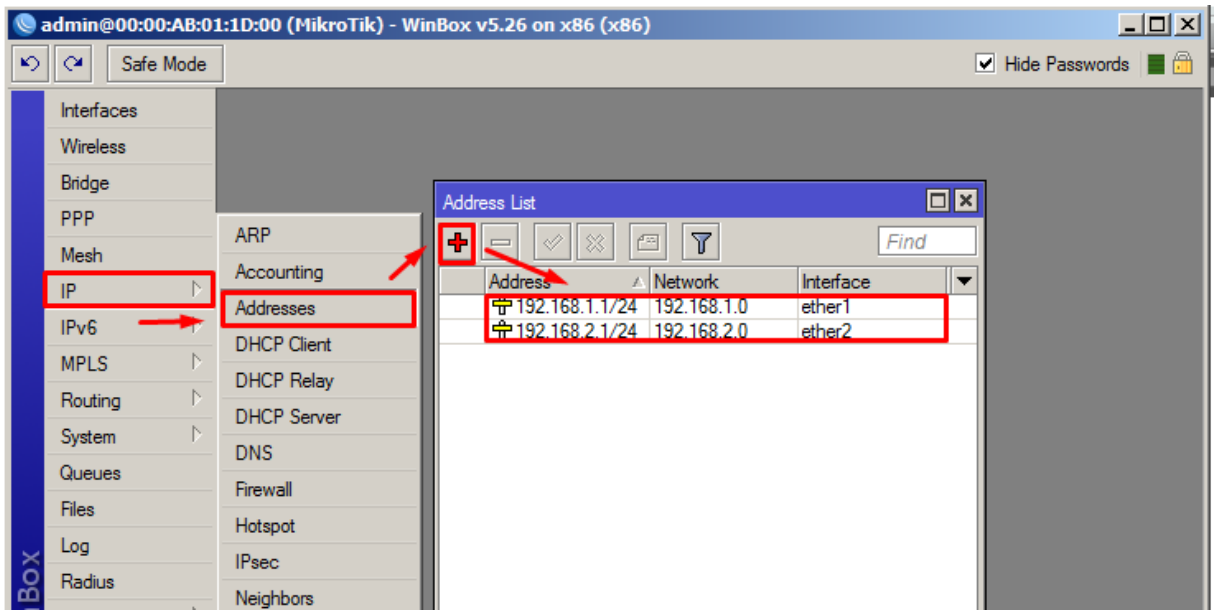
- ip address add address=192.168.1.1/24 inteface=ether1 (*Laptop Kita*)
- ip address add address=192.168.2.1/24 inteface=ether2 (*Virtual PC*)

Jalankan **Winbox** dan masuk menggunakan IP Address → **Connect**



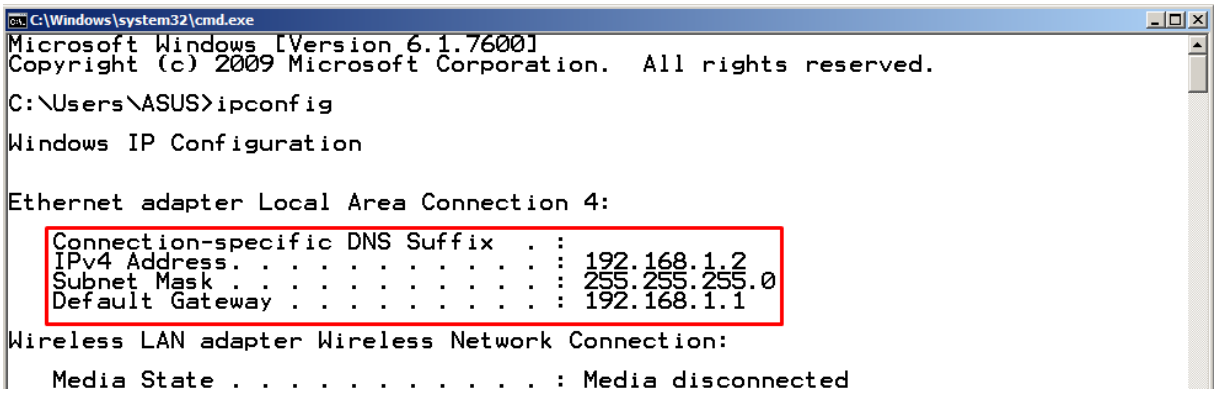


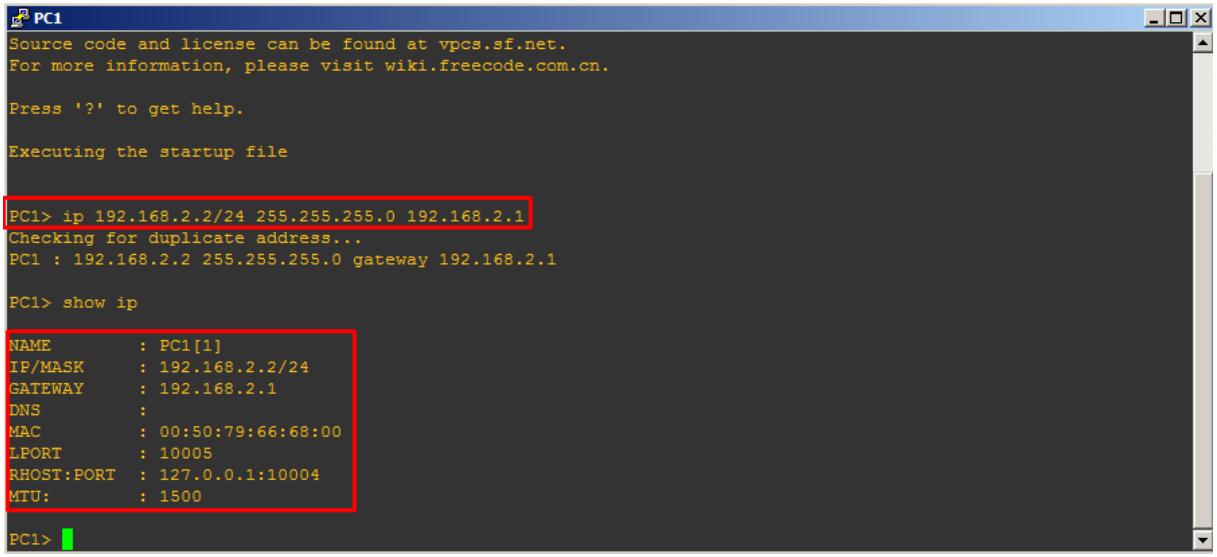
Cek IP Address = **IP → Address → IP dan Interface** harus sesuai



Isikan **IP address** pada **Loopback adapter (PC)** = 192.168.1.2/24 dan Gateway = 192.168.1.1

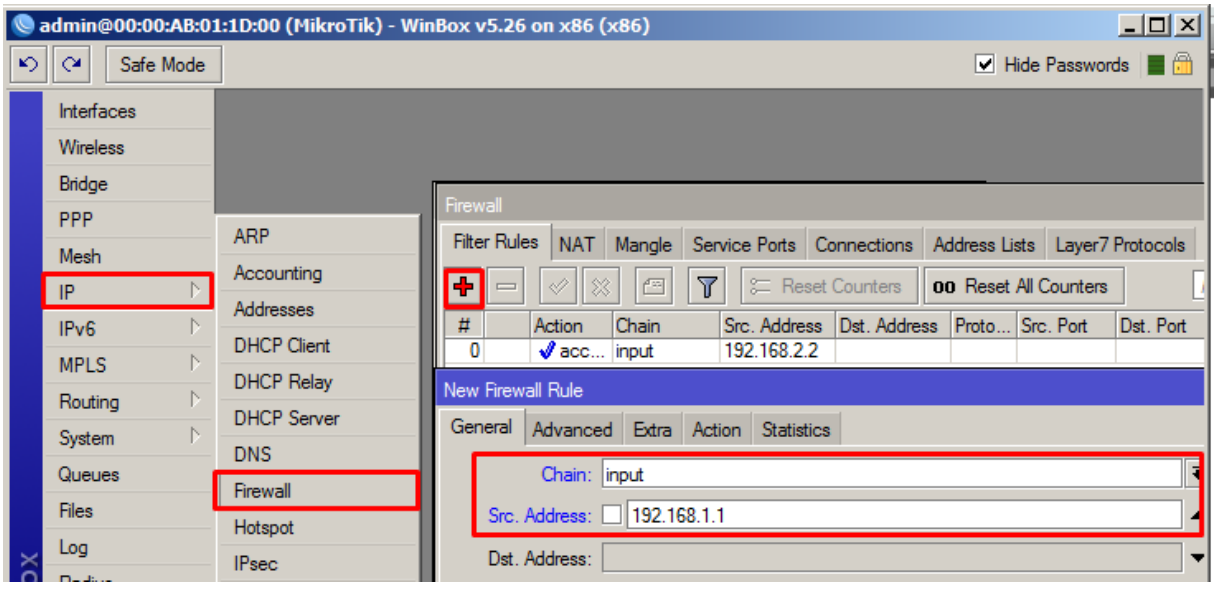
Isikan **IP address** pada **PC Virtual** = 192.168.2.2/24 Gateway = 192.168.2.1



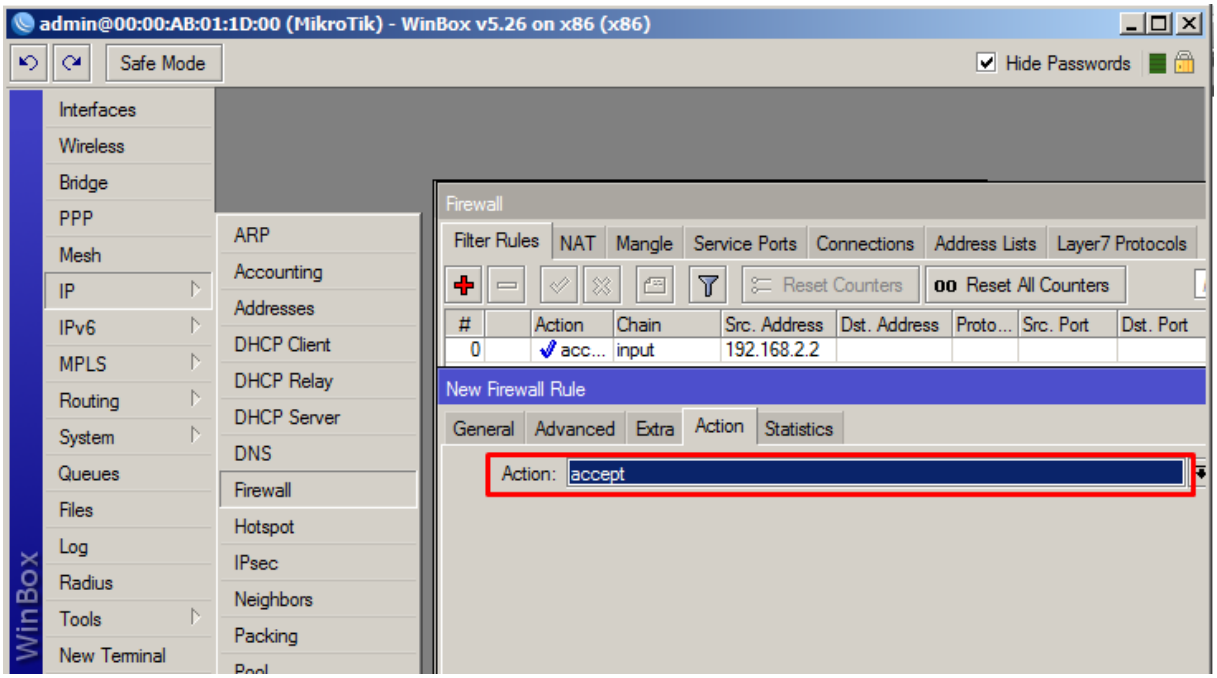


Karena kita akan membuat rule ini dengan strategi **accept few & drop any.** Berarti **chain** yang di gunakan adalah "**input**" kerena kita akan melakukan filtering traffic yang yang menuju arah router.

Masuk ke menu **IP →Firewall →filter rule →add →General**. Isikan pada **Chain : Input** karena perintah tersebut ibaratnya adalah "**JIKA** ada trafik yang menuju Router". Isikan **Src.Address=192.168.1.2** (IP PC kita), karena perintah tersebut maknanya "yang berasal dari IP".



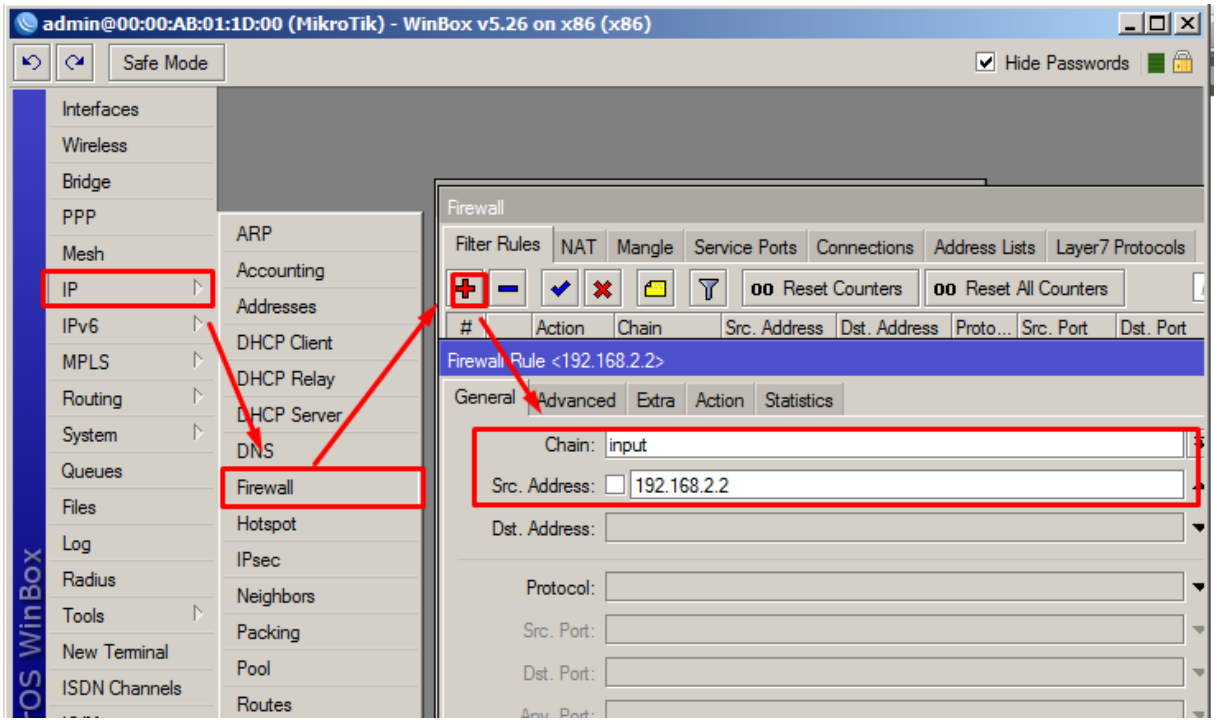
Lalu ke Tab Action, dan isikan **Action=accept.** Dalam hal ini ibaratnya "maka yang dilakukan router adalah **Accept/terima**". **Apply**, dan **OK**

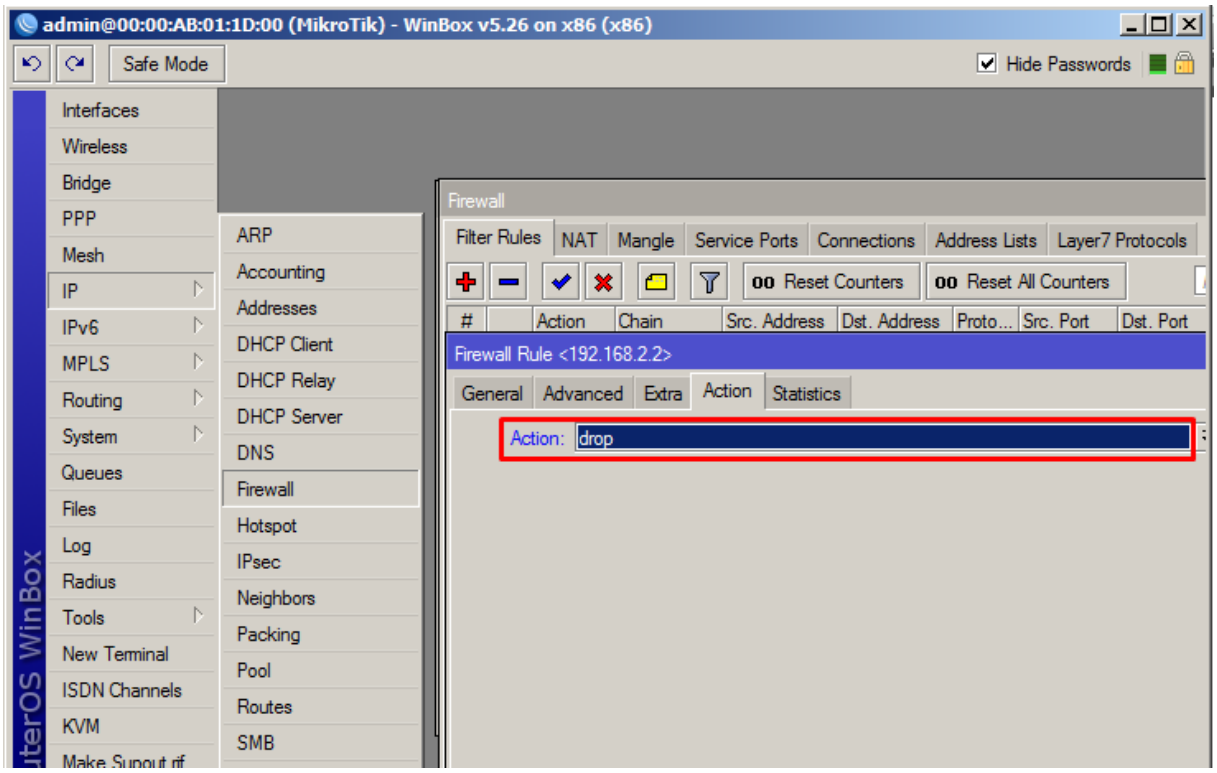


Jadi, maksud di atas adalah: jika ada yang masuk ke router dengan IP:192.168.1.2, maka router akan menerimanya" .

Barusan, kita baru saja melakukan metode yang **Accept Few** saja.

Dan sekarang kita akan membuat konsep **Drop Any.** Caranya sangat mudah, kita tinggal memasukan konfigurasi: **Chain=input** dan **Action=Drop**. Seperti gambar di bawah ini.





Lalu lihatlah di **Filter Rule**, 2 konfigurasi yang kita lakukan ada atau tidak ? dan perhatikan apakah jumlah setiap byte pada filter rule bertambah ?

Untuk test hasilnya, cobalah tancapkan PC/Laptop yang lain ke Routerboard anda, dan cobalah untuk masuk melalui **Winbox** bisa atau tidak? atau cobalah dengan mengetest dengan ping ke router, apakah bisa ?

Kemudian cobalah dengan mengetest dengan ping dari Virtual PC ke router, apakah bisa?

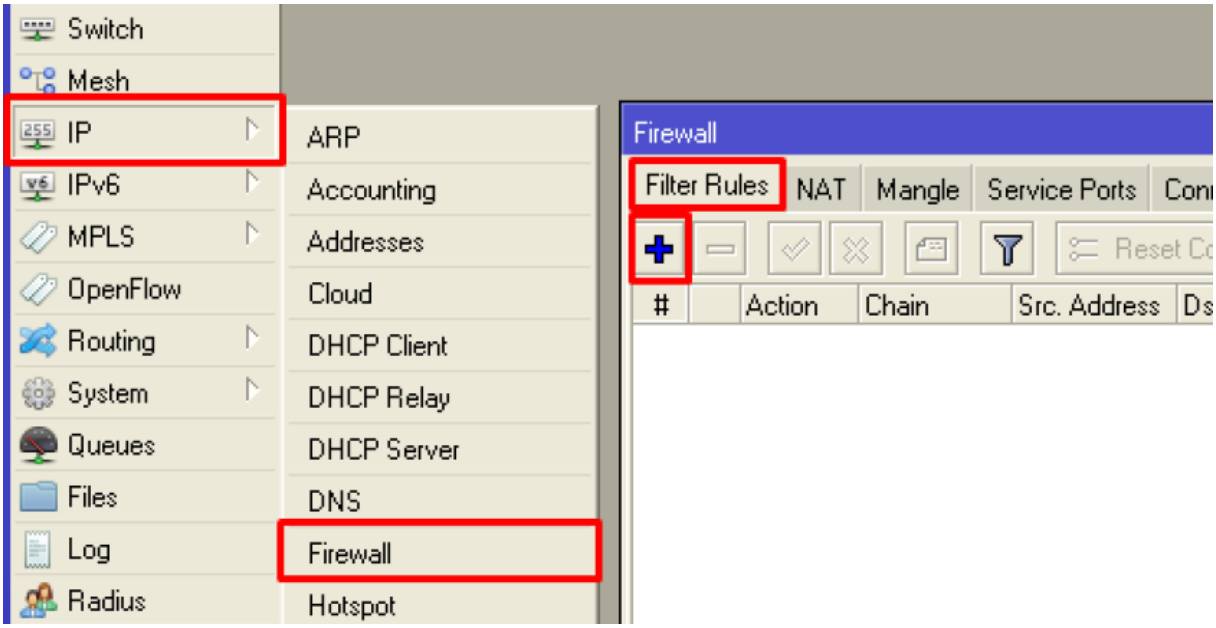
Lab

Blok Konten Dalam MikroTik

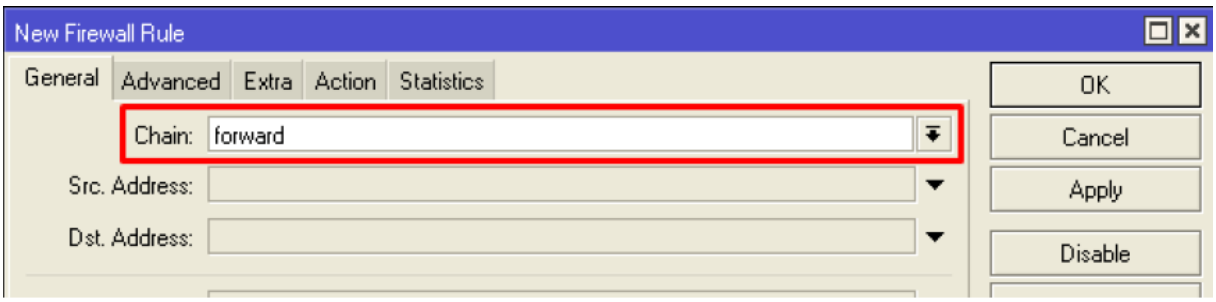
Jika kita punya router MikroTik lalu kita menjadikannya Hotspot, lalu Hotspot tersebut bisa digunakan siapapun (umum), baik anak-anak maupun orang tua ? yang namanya internet apapun ada, dari yang halal sampe yang haram pun ada, dari yang positif sampai yang negative, lalu, bagaimana jika ada anak kecil yang tak sengaja membuka situs porno gara-gara mereka menulis kata-kata yang berbau porno ? jelas bahaya kan ? yang namanya anak kan harus di didik sebaik mungkin. Maka dari itu, kita sebagai engineer, harus pintar-pintar untuk menghindari kasus-kasus tersebut, dan dalam kesempatan ini kita akan memblokir konten yang berbau Porno di mikrotik.

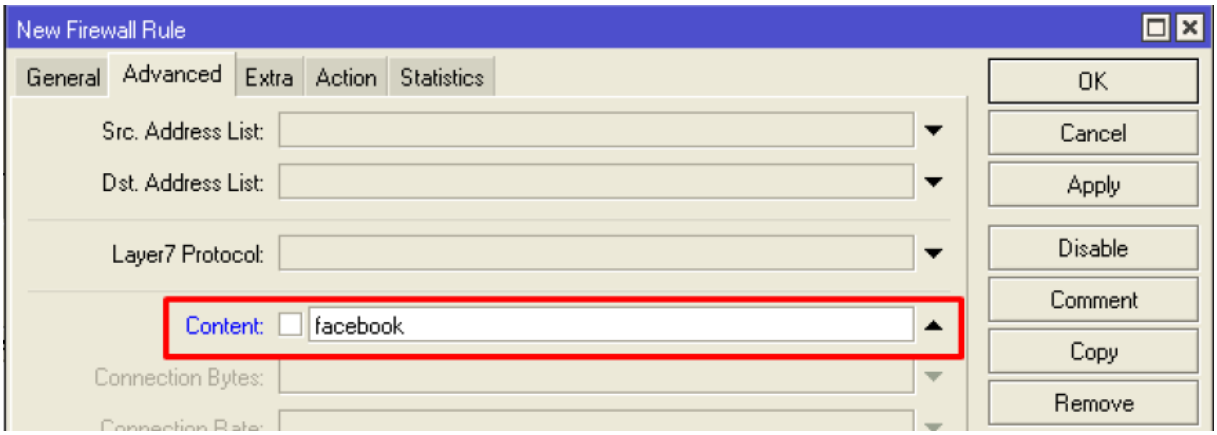
Sebelumnya. dalam praktek ini, kita akan memblokir 3 konten besar (untuk contoh saja), yaitu: **Facebook, Twitter,** dan **Porno.**

1. Siapkan mikrotik anda dan PC anda.
2. Koneksikan PC anda ke internet melalui MikroTik.
3. Masuklah ke Menu **IP>Firewall>Filter Rules> add**

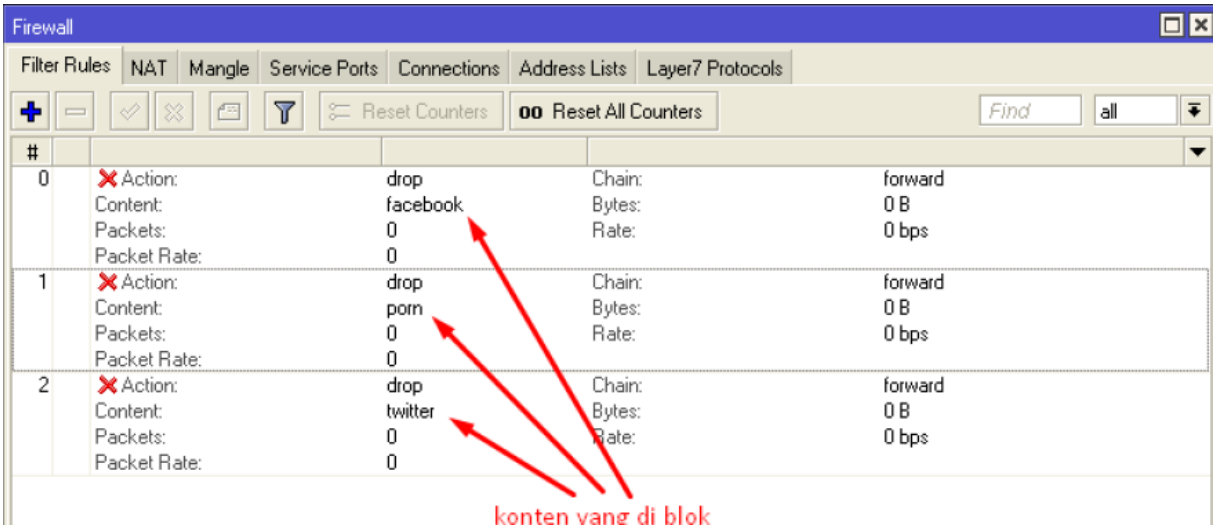


Lalu di **General,** isi **Chain=forward**, Lalu Tab ke **Advanced** dan isi di **Content=facebook,** lalu di **Action** isi dengn **Action=drop.**lalu Apply dan OK





Ulangi langkah 4 dengan Content=**Twitter** dan juga **Porn**, sehingga di filter rules terdapat 3 content yang di drop/di tolak



Cobalah **Client** untuk membuka ke 3 konten tersebut, apakah kita masih bisa masuk atau tidak ?