MUM

MikroTik User Meeting in Indonesia
Jakarta, October 20-21, 2012

SIMPLE FIREWALL

Firewall sederhana untuk memblokir akses yang tidak di ijinkan yang datang dari arah Interface Public (Wan / Internet)

Jakarta, 21 Oktober 2012

By : Adhie Lesmana
(adhielesmana)

MUM

MikroTik User Meeting in Indonesia
Jakarta, October 20-21, 2012

Speaker Profile :

* Name : - **Adhie Lesmana** (*adhielesmana*) – Solo ,Jawa Tengah
  * *Use Mikrotik Since 2008*
* Now Active :
  - **IT Staff** | at **PT.BPR SABAR ARTHA PALUR** (*Banking Business*)
  - **Network Adm** | at **Netspot Bromindo** (*local WISP Solo*)
  - **Trainer** | at **Adhie Lesmana Networking Center**
    (*Basic Network Training, TCP/IP, Routing, etc*)
  - **Member and Super Moderator :**
    at **Forum Mikrotik Indonesia (www.forummikrotik.com)**
  - **Member and Regular Moderator :**
    at **Forum TP-Link Indonesia (www.forumtplink.com)**
  - **And Many Networking Activity Other**
    Based On Maintenance and Service Job ☺

* Website : ***www.adhielesmana.com***

twitter : adhielesmana | ym : adhie_lesmana@yahoo.com
phone : 0857 – 4191 – 8585 / 0271- 255-00-55

AdhielesmanA
Your Best Networking Partner

MikroTik User Meeting in Indonesia
Jakarta, October 20-21, 2012

Forum *MikroTIK* Indonesia [FMI]

http://www.forummikrotik.com

FMI Founded By **Akbar Azwir** in June 2007
Build Using licensed **vBulletin**
Until Oktober 2012, we have **44.817** Registered Member
with **21.230** Active Member.

Here is FMI Feature :

- Wiki FMI
- Online Test
- Free Login Page Hotspot Design
- *MikroTIK* Technical Review
- Tutorial and Sharing Article's
- Searching with Prefix Sorting
- Sale And Buy Sub Forum.

AdhielesmanA
Your Best Networking Partner

MUM

MikroTik User Meeting in Indonesia
Jakarta, October 20-21, 2012

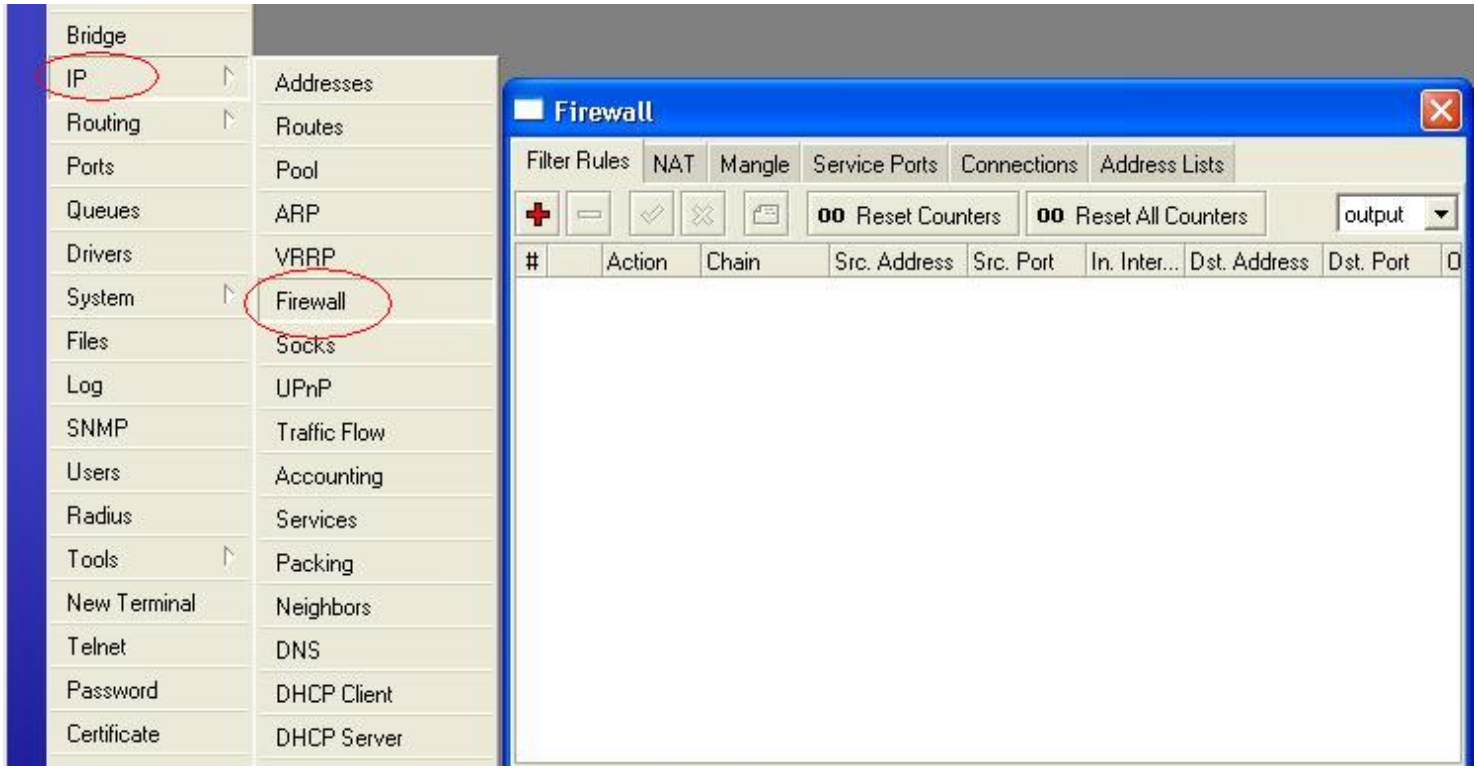
SIMPLE FIREWALL

Deskripsi :

Firewall Sederhana, yang di gunakan untuk menghalau (mem-blokir) akses yang tidak di ijinkan yang datang dari arah interface publik menuju router. selain akses -akses yang telah diijinkan,semua akses yang masuk dari interface publik (wan) akan di drop.

Original Thread : *http://www.forummikrotik.com/firewall/11755-simple-firewall-ampuh.html*

- Menggunakan Menu > IP > Firewall > Filter :



Topologi Jaringan :

Wan : - Interface ke arah internet.
Lan : - Interface ke arah lan / local.

* Secara Mudah, Untuk memblokir semua akses yang masuk dari interface wan, kita tinggal membuat rule filter dengan parameter sebagai berikut :

- chain = input
- in-interface = wan (interface ke arah internet)
- action = drop

script command :

*/ip firewall filter add chain=input in-interface=*wan action=drop*

note :

input** - used to **process packets entering the router through one of the interfaces** with the destination IP address which is one of the router's addresses. **Packets passing through the router are not processed against the rules of the input chain

**input : memproses semua akses (packet) yang masuk menuju router*

* Namun rule diatas malah menimbulkan masalah baru, yakni router tidak dapat melakukan PING, Request DNS dan Update NTP untuk kepentingan router itu sendiri. bahkan tidak bisa diremote dari outside network (internet)

Lantas Bagaimana Solusinya, Supaya Bisa menutup semua port yang tidak digunakan dan hanya mengijinkan port tertentu??

* Solusinya, Kita definisikan dan kita tentukan dulu port – port yang akan kita ijinkan, lalu kita buat rule yang mengijinkan akses masuk dari port – port yang kita ijinkan tersebut, selanjutnya kita blok akses yang masuk yang tidak kita kenal.

* Buat dulu rule rule untuk mengijinkan packet tertentu.

1. Ijinkan Remoting Winbox dari Outside Network
/Ip firewall filter add **chain**=input **in-interface**=**wan* **protocol**=tcp **dst-port**=8291 **action**=accept **comment**="Allow Remote winbox dari Publik" **disabled**=no

2. Ijinkan NTP Update
/Ip firewall filter add **chain**=input **in-interface**=**wan* **protocol**=tcp **src-port**=123 **action**=accept **comment**="Allow NTP Update " **disabled**=no

3. Ijinkan DNS Request
/Ip firewall filter add **chain**=input **in-interface**=**wan* **protocol**=udp **src-port**=53 **action**=accept **comment**="Allow Request DNS" **disabled**=no

4. Ijinkan ICMP Traffic Menuju Router (Ping, Traceroute dll)
/Ip firewall filter add **chain**=input **in-interface**=**wan* **protocol**=icmp **action**=accept **comment**="Allow ICMP Traffic" **disabled**=no

* Lalu Untuk Memblokir Lainya :

5. Catat IP unauthorized yang mencoba berkoneksi
/Ip firewall filter add **chain**=input **in-interface**=**wan* **connection-state**=new **action**=add-src-to-address-list **address-list**=spam **address-list-timeout**=30m **comment**="Log Ip Yang Di Tolak" **disabled**=no

6. Drop Semua Akses yang tidak di ijinkan
/Ip firewall filter add **chain**=input **in-interface**=**wan* **action**=drop **comment**="Drop Semua Akses yang tidak di ijinkan" **disabled**=no

* Secara ajaib packet yang masuk menuju router dari arah publik akan di drop oleh mikrotik, kecuali trafic – traffic paket yang sudah kita ijinkan di rule sebelumnya.

* fungsi rule nomor 5 tidak berhubungan dengan fungsi rule nomor 6, karena rule nomor 5 hanya mencatat ip sumber dan menuliskannya dalam firewall address list (menu > ip > firewall > address list)

* fungsi rule nomor 6 digunakan untuk men-drop (mengeliminiasi / memblokir) akses – akses yang mencoba berkomunikasi dengan router selain akses yang telah di ijinkan.

* Perhatian, berhati hati lah pada penempatan rule, karena penempatan rule pada filter rule membaca rule paling atas lebih dulu, apabila penempatan rule **drop** di pasang pada rule paling atas, maka rule rule dibawahnya, meski di **accept** tetap tidak akan bisa mengakses karena telah di drop lebih dulu.

* Disarankan melakukan setting dengan anda berada di local area (lan) dari router tersebut, karena apabila dilakukan setting via remote dari outside network, apabila tidak cermat dan tidak teliti dapat mengakibatkan router tidak dapat diremote dari jaringan luar, port winbox pada rule firewall wajib di sesuaikan dengan kondisi port winbox yang diseting pada router tersebut.

* Perhatian, Rule ini tidak menyebabkan nge-lag, lelet, lemot, gangguan jaringan, dan kelambatan bandwith pada klien.. Karena ini hanya rule firewall terhadap router, tidak mengatur bandwith maupun mengatur firewall terhadap klien.

* Pengaturan Pengamanan dan firewall terhadap klien atau interface di sisi local pada umumnya hampir serupa, tinggal dilakukan custom baik chain, port maupun protocolnya.. namun kesemuanya itu tidak akan dibahas kali ini, kita tunggu saja di MUM Tahun depan ☺…

* Selesai…….

MUM

MikroTik User Meeting in Indonesia
Jakarta, October 20-21, 2012

* Thanks To :
- **Mikro*TIK*, Routerboard**, with All Staff and Engineer
- **MUM 2012** and All Participant's (tenant, sponsor and guest)
- **Mr. Valens Riyadi** and Citraweb (www.mikrotik.co.id)

*And Specialy Thanks To :
- **Forum Mikrotik Indonesia** with All Member and Forum Management
- **DCSindo**, **Spektrum** and Any Forum Partnership
- **FMI Regional Solo** our Home Land
- All Client, Member and Partner **Adhielesmana**

*Warm Regards

Adhie Lesmana

AdhielesmanA
Your Best Networking Partner

Q & A

AdhielesmanA
Your Best Networking Partner