

Firewall untuk router mikrotik

Contributed by harijanto@datautama.net.id
 Thursday, 09 November 2006
 Last Updated Wednesday, 03 January 2007

Untuk mengamankan router mikrotik dari traffic virus dan excess ping dapat digunakan skrip firewall berikut

Pertama buat address-list "ournetwork" yang berisi alamat IP radio, IP LAN dan IP WAN atau IP lainnya yang dapat dipercaya

Dalam contoh berikut alamat IP radio adalah = 10.0.0.0/16, IP LAN = 192.168.2.0/24 dan IP WAN = 203.89.24.0/21 dan IP lainnya yang dapat dipercaya = 202.67.33.7

Untuk membuat address-list dapat menggunakan contoh skrip seperti berikut ini tinggal disesuaikan dengan konfigurasi jaringan Anda.

Buat skriptip berikut menggunakan notepad kemudian copy-paste ke console mikrotik

```
/ ip firewall address-list
add list=ournetwork address=203.89.24.0/21 comment="Datautama Network" \
  disabled=no
add list=ournetwork address=10.0.0.0/16 comment="IP Radio" disabled=no
add list=ournetwork address=192.168.2.0/24 comment="LAN Network" disabled=no
```

Selanjutnya copy-paste skrip berikut pada console mikrotik

```
/ ip firewall filter
add chain=forward connection-state=established action=accept comment="allow \
  established connections" disabled=no
add chain=forward connection-state=related action=accept comment="allow \
  related connections" disabled=no
add chain=virus protocol=udp dst-port=135-139 action=drop comment="Drop \
  Messenger Worm" disabled=no
add chain=forward connection-state=invalid action=drop comment="drop invalid \
  connections" disabled=no
add chain=virus protocol=tcp dst-port=135-139 action=drop comment="Drop \
  Blaster Worm" disabled=no
add chain=virus protocol=tcp dst-port=1433-1434 action=drop comment="Worm" \
  disabled=no
add chain=virus protocol=tcp dst-port=445 action=drop comment="Drop Blaster \
  Worm" disabled=no
add chain=virus protocol=udp dst-port=445 action=drop comment="Drop Blaster \
  Worm" disabled=no
add chain=virus protocol=tcp dst-port=593 action=drop comment="_____ " \
  disabled=no
add chain=virus protocol=tcp dst-port=1024-1030 action=drop comment="_____ " \
  disabled=no
add chain=virus protocol=tcp dst-port=1080 action=drop comment="Drop MyDoom" \
  disabled=no
add chain=virus protocol=tcp dst-port=1214 action=drop comment="_____ " \
  disabled=no
add chain=virus protocol=tcp dst-port=1363 action=drop comment="ndm requester" \
  disabled=no
add chain=virus protocol=tcp dst-port=1364 action=drop comment="ndm server" \
  disabled=no
add chain=virus protocol=tcp dst-port=1368 action=drop comment="screen cast" \
  disabled=no
add chain=virus protocol=tcp dst-port=1373 action=drop comment="hromgrafx" \
  disabled=no
add chain=virus protocol=tcp dst-port=1377 action=drop comment="cichlid" \
  disabled=no
add chain=virus protocol=tcp dst-port=2745 action=drop comment="Bagle Virus" \
```

```
disabled=no
add chain=virus protocol=tcp dst-port=2283 action=drop comment="Drop Dumaru.Y" \
disabled=no
add chain=virus protocol=tcp dst-port=2535 action=drop comment="Drop Beagle" \
disabled=no
add chain=virus protocol=tcp dst-port=2745 action=drop comment="Drop \
Beagle.C-K" disabled=no
add chain=virus protocol=tcp dst-port=3127 action=drop comment="Drop MyDoom" \
disabled=no
add chain=virus protocol=tcp dst-port=3410 action=drop comment="Drop Backdoor \
OptixPro" disabled=no
add chain=virus protocol=tcp dst-port=4444 action=drop comment="Worm" \
disabled=no
add chain=virus protocol=udp dst-port=4444 action=drop comment="Worm" \
disabled=no
add chain=virus protocol=tcp dst-port=5554 action=drop comment="Drop Sasser" \
disabled=no
add chain=virus protocol=tcp dst-port=8866 action=drop comment="Drop Beagle.B" \
disabled=no
add chain=virus protocol=tcp dst-port=9898 action=drop comment="Drop \
Dabber.A-B" disabled=no
add chain=virus protocol=tcp dst-port=10000 action=drop comment="Drop \
Dumaru.Y, sebaiknya di disable karena juga sering digunakan utk vpn atau \
webmin" disabled=yes
add chain=virus protocol=tcp dst-port=10080 action=drop comment="Drop \
MyDoom.B" disabled=no
add chain=virus protocol=tcp dst-port=12345 action=drop comment="Drop NetBus" \
disabled=no
add chain=virus protocol=tcp dst-port=17300 action=drop comment="Drop Kuang2" \
disabled=no
add chain=virus protocol=tcp dst-port=27374 action=drop comment="Drop \
SubSeven" disabled=no
add chain=virus protocol=tcp dst-port=65506 action=drop comment="Drop PhatBot, \
Agobot, Gaobot" disabled=no
add chain=forward action=jump jump-target=virus comment="jump to the virus \
chain" disabled=no
add chain=input connection-state=established action=accept comment="Accept \
established connections" disabled=no
add chain=input connection-state=related action=accept comment="Accept related \
connections" disabled=no
add chain=input connection-state=invalid action=drop comment="Drop invalid \
connections" disabled=no
add chain=input protocol=udp action=accept comment="UDP" disabled=no
add chain=input protocol=icmp limit=50/5s,2 action=accept comment="Allow \
limited pings" disabled=no
add chain=input protocol=icmp action=drop comment="Drop excess pings" \
disabled=no
add chain=input protocol=tcp dst-port=21 src-address-list=ournetwork \
action=accept comment="FTP" disabled=no
add chain=input protocol=tcp dst-port=22 src-address-list=ournetwork \
action=accept comment="SSH for secure shell" disabled=no
add chain=input protocol=tcp dst-port=23 src-address-list=ournetwork \
action=accept comment="Telnet" disabled=no
add chain=input protocol=tcp dst-port=80 src-address-list=ournetwork \
action=accept comment="Web" disabled=no
add chain=input protocol=tcp dst-port=8291 src-address-list=ournetwork \
action=accept comment="winbox" disabled=no
add chain=input protocol=tcp dst-port=1723 action=accept comment="pptp-server" \
disabled=no
add chain=input src-address-list=ournetwork action=accept comment="From \
Datautama network" disabled=no
add chain=input action=log log-prefix="DROP INPUT" comment="Log everything \
else" disabled=no
add chain=input action=drop comment="Drop everything else" disabled=no
```

Efek dari skrip diatas adalah:

- router mikrotik hanya dapat diakses FTP, SSH, Web dan Winbox dari IP yang didefinisikan dalam address-list "ournetwork" sehingga tidak bisa diakses dari sembarang tempat.
- Port-port yang sering dimanfaatkan virus di blok sehingga traffic virus tidak dapat dilewatkan, tetapi perlu diperhatikan jika ada user yang kesulitan mengakses service tertentu harus dicek pada chain="virus" apakah port yang dibutuhkan user tersebut terblok oleh firewall.
- Packet ping dibatasi untuk menghindari excess ping.

Selain itu yang perlu diperhatikan adalah: sebaiknya buat user baru dan password dengan group full kemudian disable user admin, hal ini untuk meminimasi resiko mikrotik Anda di hack orang.

Selamat mencoba