[Setting Firewall MikrotikRouterOS](http://degeul.byethost7.com/?p=14" \o "Permanent Link to Setting Firewall MikrotikRouterOS)  
08 17th, 2007

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

Langkah 1 :

/ ip firewall address-list add list=ournetwork address=192.168.7.0/24 comment=”LAN Network” disabled=no

Langkah 2 :

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 didisable 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=”SMANELA 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

Kemudian tinggal di sesuaikan dengan konfigurasi jaringan di tempat anda, setelah itu tinggal Copy and Paste di konsol MikrotikRouterOS

Efek dari skrip diatas adalah:  
MikrotikRoutrOS 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 MikrotikRouterOS Anda di hack orang.

Selamat Mencoba dan Semoga bermanfaat.

http://degeul.byethost7.com/wp-content/themes/Tropical_Grunge/images/h_l.gif

http://degeul.byethost7.com/wp-content/themes/Tropical_Grunge/images/showpost.gif[Read Comments(0)](http://degeul.byethost7.com/?p=14#comments)

http://degeul.byethost7.com/wp-content/themes/Tropical_Grunge/images/fl.gif[Membuat Gateway dengan Mikrotik](http://degeul.byethost7.com/?p=5)  
06 12th, 2007

Berikut ini adalah langkah dasar setup mikrotik yang dikonfigurasikan sebagai gateway dalam jaringan (berdasarkan pengalaman saya)

1. Langkah pertama adalah install Mikrotik RouterOS pada PC.  
Untuk lebih amannya pilih semua dengan menekan tombol ‘a’ di keyboard pada saat pemilihan software apa saja yang akan di install

2. Login Pada Mikrotik Routers melalui console :  
MikroTik v2.9.6  
Login: admin [enter]  
Password: (kosongkan) [enter]

#Sampai langkah ini kita sudah bisa masuk pada mesin Mikrotik. User default adalah admin  
dan tanpa password, tinggal ketik admin kemudian tekan tombol enter.

3. Untuk keamanan, disarankan untuk mengganti password terlebih dahulu  
!!! Semua password ditandai dengan simbol asterik(\*)  
[admin@Mikrotik] > password  
old password: \*\*\*\*\* [enter] #tekan enter  
new password: \*\*\*\*\* [enter] #masukkan PAssword yang dikehendaki  
retype new password: \*\*\*\*\* [enter] #masukkan lagi password sama dengan di atas  
[admin@ Mikrotik] >

4. Mengganti nama Mikrotik, pada langkah ini nama identitas server akan diganti menjadi â€œgugunâ€  
[admin@Mikrotik] > system identity set name=gugun [enter]  
[admin@gugun] >

5. Melihat NIC yang terdapat di CPU  
[admin@gugun] > interface print [enter]  
Flags: X - disabled, D - dynamic, R - running  
# NAME TYPE RX-RATE TX-RATE MTU  
0 R ether1 ether 0 0 1500  
1 R ether2 ether 0 0 1500  
[admin@gugun] >

Artinya ada dua NIC dengan nama ether1 dan ether2

6. Memberikan IP address pada tiap NIC. Misalkan ether1 akan kita gunakan untuk koneksi ke Internet dengan IP 10.42.1.15 dan ether2 akan kita gunakan untuk LAN kita dengan IP 19.15.1.254

[admin@gugun] > ip address add address=10.42.1.15/24 interface=ether1 [enter]  
[admin@gugun] > ip address add address=19.15.1.254/24 interface=ether2 [enter]

Penulisan xxx.xxx.xxx.xxx/24 dapat diartikan bahwa netmask IP tersebut adalah 255.255.255.0, penulisan bisa diganti seperti di bawah ini  
[admin@gugun] > ip address add address=10.42.1.15 netmask=255.255.255.0 interface=ether1  
Dst..

7. Melihat konfigurasi IP address yang sudah kita berikan  
[admin@gugun] >ip address print [enter]  
Flags: X - disabled, I - invalid, D - dynamic  
# ADDRESS NETWORK BROADCAST INTERFACE  
0 10.42.1.15 10.42.1.0 10.42.1.255 ether1  
1 19.15.1.254 19.15.1.0 19.15.1.255 ether2  
[admin@gugun] >

8. Memberikan default Gateway  
Diasumsikan gateway untuk koneksi internet adalah 10.42.1.254  
[admin@gugun] > /ip route add gateway=10.42.1.254 [enter]

9. Melihat Tabel routing pada Mikrotik  
[admin@gugun] > ip route print [enter]  
Flags: X - disabled, A - active, D - dynamic,  
C - connect, S - static, r - rip, b - bgp, o - ospf  
# DST-ADDRESS PREFSRC G GATEWAY DISTANCE INTERFACE  
0 ADC 19.15.0.0/24 19.15.1.254 ether2  
1 ADC 10.42.0.0/26 10.42.1.15 ether1  
2 A S 0.0.0.0/0 r 10.42.1.254 ether1  
[admin@gugun] >

10. Lakukan test koneksi ke default gateway untuk memastikan bahwa koneksi sudah benar  
[admin@gugun] > ping 10.42.1.254 [enter]  
10.42.1.254 64 byte ping: ttl=64 time<1 ms  
10.42.1.254 64 byte ping: ttl=64 time<1 ms  
2 packets transmitted, 2 packets received, 0% packet loss  
round-trip min/avg/max = 0/0.0/0 ms  
[admin@gugun] >

Untuk menghentikan proses tekan kombinasi Ctrl+C

11. Seting DNS pada Mikrotik  
[admin@gugun] > ip dns set primary-dns=10.42.1.1 allow-remoterequests=no [enter]  
[admin@gugun] > ip dns set secondary-dns=202.134.1.10 allow-remoterequests=no [enter]

12. Melihat konfigurasi DNS  
[admin@gugun] > ip dns print [enter]  
primary-dns: 10.42.1.1  
secondary-dns: 202.134.1.10  
allow-remote-requests: no  
cache-size: 2048KiB  
cache-max-ttl: 1w  
cache-used: 16KiB  
[admin@gugun] >

13. Lakukan pengecekan koneksi ke internet, Misal google.com  
[admin@gugun] > ping www.google.com [enter]  
66.249.89.104 64 byte ping: ttl=235 time=160 ms  
66.249.89.104 64 byte ping: ttl=235 time=148 ms  
66.249.89.104 64 byte ping: ttl=235 time=153 ms  
66.249.89.104 64 byte ping: ttl=235 time=144 ms  
4 packets transmitted, 4 packets received, 0% packet loss  
round-trip min/avg/max = 144/151.2/160 ms

Jika hasilnya reply berarti seting DNS sudah benar.

14. Lakukan seting Masqurading  
[admin@gugun]> ip firewall nat add action=masquerade outinterface=  
ether1 chain:srcnat [enter]

15. Melihat konfigurasi Masquerading  
[admin@gugun]ip firewall nat print [enter]  
Flags: X - disabled, I - invalid, D - dynamic  
0 chain=srcnat out-interface=ether1 action=masquerade  
[admin@gugun] >

Setelah langkah ini bisa dilakukan pemeriksaan untuk koneksi dari jaringan local. Dan jika berhasil berarti kita sudah berhasil melakukan instalasi Mikrotik Router sebagai Gateway server. Setelah terkoneksi dengan jaringan Mikrotik dapat dimanage menggunakan WinBox  
yang bisa di download dari Mikrotik.com atau dari server mikrotik kita.

Misal Ip address server  
mikrotik kita 19.15.1.254, via browser buka http://19.15.1.254 dan download WinBox dari situ.  
Jika kita menginginkan client mendapatkan IP address secara otomatis maka perlu kita setup dhcp server pada Mikrotik. Berikut langkah-langkahnya :

1.Buat IP address pool  
/ip pool add name=dhcp-pool ranges=19.15.1.10-19.15.1.20

2. Tambahkan DHCP Network dan gatewaynya yang akan didistribusikan ke client Pada contoh ini networknya adalah 19.15.0.0/24 dan gatewaynya 19.15.1.1  
/ip dhcp-server network add address=19.15.0.0/24 gateway=19.15.1.1

3. Tambahkan DHCP Server ( pada contoh ini dhcp diterapkan pada interface ether2 )  
/ip dhcp-server add interface=ether2 address-pool=dhcp-pool

4. Lihat status DHCP server  
[admin@gugun]> ip dhcp-server print [enter]  
Flags: X - disabled, I - invalid  
# NAME INTERFACE RELAY ADDRESS-POOL LEASE-TIME ADD-ARP  
0 X dhcp1 ether2  
Tanda X menyatakan bahwa DHCP server belum enable maka perlu dienablekan terlebih dahulu pada langkah 5.

5. Jangan Lupa dibuat enable dulu dhcp servernya  
/ip dhcp-server enable 0

kemudian cek kembali dhcp-server seperti langkah 4, jika tanda X sudah tidak ada berarti sudah aktif.

6. Tes Dari client di command prompt  
c:\>ping www.google.com [enter]

untuk bandwith controller, bisa dengan sistem simple queue ataupun bisa dengan mangle  
[admin@gugun] queue simple> add name=Komputer01  
interface=ether2 target-address=19.15.1.10/24 max-limit=65536/131072  
[admin@gugun] queue simple> add name=Komputer02  
interface=ether2 target-address=19.15.1.11/24 max-limit=65536/131072  
dan seterusnyaâ€¦