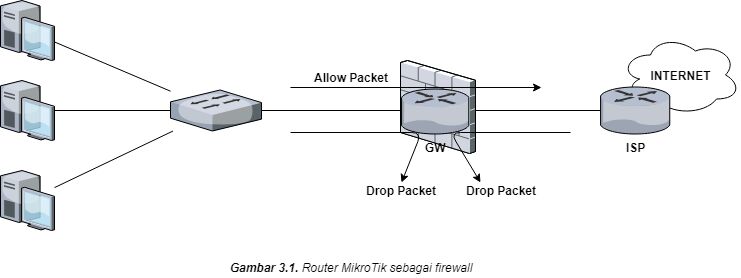
Firewall merupakan perangkat yang berfungsi untuk memeriksa dan menentukan paket data yang dapat keluar atau masuk dari sebuah jaringan. Dengan kemampuan menentukan apakah sebuah paket data bisa masuk dan keluar dari suatu jaringan maka firewall berperan untuk melindungi jaringan dari serangan yang berasal dari jaringan luar (outside network). Misalnya difungsikan untuk melindungi jaringan lokal (LAN) dari kemungkinan serangan yang berasal dari internet. Selain ditujukan untuk melindungi jaringan, firewall juga dapat difungsikan untuk melindungi sebuah komputer user atau host (single host), firewall jenis ini disebut host firewall.

Jika kembali melihat skenario awal yang ada di Bab 2, maka Router Mikrotik Anda akan berfungsi sebagai firewall. Router ini berada di antara jaringan lokal 10.10.10.0/24 dengan jaringan internet dan akan bertugas melindungi jaringan lokal tersebut. Router Mikrotik ini akan berfungsi menentukan jenis paket data apa yang diizinkan menuju internet, dan menentukan paket data apa yang dapat masuk ke jaringan lokal Anda.



Untuk mempelajari firewall secara mendalam,Anda seharusnya sudah memiliki pengetahuan tentang IP Packet, misalnya informasi IP Address pengirim(source address),IP Address tujuan (destiniation address),Port Pengirim(source port),Port Tujuan (destination port).Anda juga sebaiknya memiliki pengetahuan tentang jenis protokol yang digunakan oleh berbagai aplikasi Internet,apakah aplikasi tersebut mengunakan TCP atau UDP bahkan ICMP.

Saya tidak akan membahas tentang bagaimana melihat parameter-parameter apa yang ada di suatu IP packet.Anda dapat membaca buku-buku yang khusus membahas tentang TCP/IP. Namun jika Anda pun belum menguasai ilmu TCP/IP, saya berusaha membuat buku ini mudah dimenegerti. Saya berusaha menjadikan buku ini sebagai panduan praktis bagi Anda yang baru mulai menggunalan Router Mikrotik.Saya tidak ingin anda mundur menggunakan RouterMikrotik hanya karena belum menguasai benar ilmu TCP/IP.

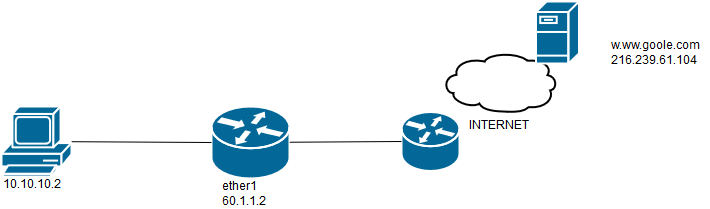
Pada Bab 3 ini,saya akan membahas dua fitur yang ada di firewall Routter Mikrotik, yaitu Network Translation (NAT) dan Filter. *Network Address Translation* akan bertugas melakukan perubahan IP Packet yang akan dikirimkan ke Internet. Fitur-Fitur akan bertugas memeriksa pakaet data yang ditujukan bagi Router Mikrotik itu sendir. Router Mikrotik juga harus mampu mengamankan dirinya sendiri,selain tugas utamanya mengamankan jaringan. Bagaimana mungkin mengamankan jaringan kalau dirinya sendiri tidak mampu diamankan. Itulah fungsi Filter, yang pada buku ini akan lebih banyak digunakan untuk mengamankan router itu sendiri

**Network Address Translation**

*Network Address Translation*(NAT) adalah suatu fungsi firewall yang sebenarnya bertugas melakukan perubahan IP Addres pengirim dari sebuah paket data NAT ini umumnya dijalankan pada router-router yang menjadi batas antara jaringan lokal dan jaringan internet.Secara teknis NAT ini akan mengubah paket data yang berasal dari komputer user seolah-olah berasal dari router sebagai berikut.

|  |
| --- |
| Src IP Address : 10.10.10.2 |
| Dst. Ip Address: 216.239.61.104 |
| Data : HTTP Request |

|  |
| --- |
| Src IP Address : 60.1.1.2 |
| Dst. Ip Address: 216.239.61.104 |
| Data : HTTP Request |



*Gambar 3.2. NAT yang merubah IP Address pengirim*

Pada skenario jaringan di buku ini, Router MikroTik akan menjalankan NAT dengan *action=masquerade,* sehingga mengubah semua paket data yang berasal dari komputer user seolah-olah berasal dari router yang mempunayai IP Address 60.1.1.2. Ini akan meneyababkan server-server di Internet tidak mengetahui bahwa sebenyarnya yang meng-akses mereka adalah komputer user dengan IP Address 10.10.10.2, 10.10.10.3 dan seterusnya. Server-server di Internet hanya mengertahui bahwa yang meng-akses mereka adalah router dengan IP Address 60.1.1.2. Anda harus memperhatikan dengan seksama gambar 3.2

Masquerade ini wajib diajalankan oleh router-router gateway untuk menyembunyikan IP Address Private tersebut harus disembunyikan, karena pada jaringan lokal yang lain kemungkinan IP Address 10.10.10.0/24 juga digunakan. Jika Anda tidak melakukan masquerade maka komputer user tidak akan dapat mengakses Internet.

Masquerade tadi akan menyembunyikan komputer user yang ada di jaringan lokal sekaligus membuat komputer tersebut bertopeng (ber-mask) ke IP Address 60.1.1.2. Sehingga baik komputer user 10.10.10.2,10.10.10.3,10.10.10.4 dan 10.10.10.5 akan dikenal di Internet sebagai 60.1.1.2.

Jika Anda membaca kembali Bab 2, pada sub bab Masquerade terdapat satu perintah NAT yang dapat membuat komputer user mengakses Internet. Sekedar untuk menyegarkan kembali,perintah tersebut adalah sebagai berikut.

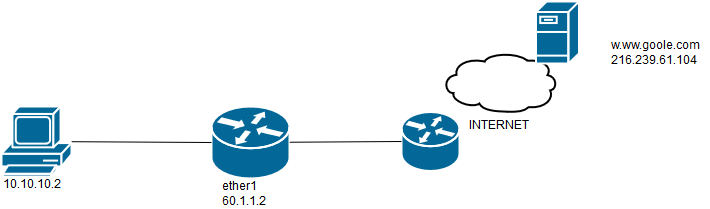
[admin@MikroTik]> **ip firewall nat add chain=srcnat**

**Out-interface=ether1 action=masquerade**

Perintah di atas adalah perintah pada firewall MikroTik yang memerintahkan “jika ada komputer user yang akan mengakses Internet, bertopenglah pada *ether1*”. Sedangkan *chain=srcnat*, berfungsi memerintahkan “gantilah IP Address pengirim(souce address) 10.10.10.2,10.10.10.3,10.10.10.4 dan 10.10.10.5 menjadi IP Address di *ether1* jika ingin menuju Internet”

|  |
| --- |
| Src IP Address : 10.10.10.2 |
| Dst. Ip Address: 216.239.61.104 |
| Data : HTTP Request |

|  |
| --- |
| Src IP Address : 60.1.1.2 |
| Dst. Ip Address: 216.239.61.104 |
| Data : HTTP Request |



*Gambar 3.3 Masquerade ke ether1*

Perintah masquerade sebelumnya tidak mencantumkan IP Address yang berhak mendapatkan akses internet, sehingga sulit membuat batasan komputer mana saja yang berhak mengakses internet. Berikut ini adalah perintah konfigurai masquerade namun disertai penambahan opsi IP address pengirim (src-address). Hanya computer yang IP Address-nya termasuk dalam opsi src-address yang akan dapat mengakses Internet. Contoh perintahnya adalah sebagai berikut :

[admin@MikroTik]> ip firewall nat add chain=srcnat

Src-address=10.10.10.0/24 out-interface=ether1 action=masquerade

[admin@MikroTik]> ip firewall nat print

Flags: X – disabled, I – invalid, D – dynamic

0 chain=srcnat action=masquerade src-address=10.10.10.0/24

out-interface=ether1

Dengan menambahkan src-address=10.10.10.0/24, berarti anda mengizinkan semua computer user di jaringan local untuk dapat mengakses Internet, baik itu computer user dengan IP Address 10.10.10.2, 10.10.10.3, 10.10.10.4 sampai dengan computer yang memiliki IP Address 10.10.10.254.

Jika Ternyata anda hanya mengizinkan empat computer user yang dapat mengakses internet (misalnya client 10.10.10.2, 10.10.10.3, 10.10.10.4, dan 10.10.10.5), maka anda dapat mengganti opsi src-address=10.10.10.0/24 dengan opsi src-address=10.10.10.2-10.10.10.5, seperti berikut ini :

[admin@MikroTik]> ip firewall nat add chain=srcnat

src-address=10.10.10.2-10.10.10.5 out-interface=ether1

action=masquerade

[admin@MikroTik]> ip firewall nat print

Flags: X – disabled, I – invalid, D – dynamic

0 chain=srcnat action=masquerade src-address=10.10.10.2-10.10.10.5

out-interface=ether1

Perlu anda ingat, jangan menumpuk konfigurasi NAT, jikan anda ingin mencoba konfigurasi di atas, maka hapuslah konfigurasi sebelumnya dengan menggunakan perintah sebagai berikut :

[admin@MikroTik]> ip firewall nat remove <nomor-index>

Jika anda menumpuk konfigurasi-konfigurasi tersebut, maka Router Mikrotik akan mengeksekusi semua baris-baris konfigurasi tersebut. Itulah sebabnya di akhir konfigurasi saya memberikan perintah ip firewall nat print untuk memastikan tidak ada konfigurasi yang tertumpuk.

Contoh berikut memperlihatkan konfigurasi NAT yang tertumpuk dan akhirnya tidak maksimal untuk menjalankan fungsi firewall. Pada contoh ini, sang Administrator jaringan menginginkan hanya computer 10.10.10.2 sampai 10.10.10.5 yang dapat mengakses internet, namun sang Administrator lupa untuk menghapus konfigurasi NAT dengan src-address=10.10.10.0/24, seperti terlihat berikut ini :

[admin@MikroTik]> ip firewall nat add chain=srcnat

src-address=10.10.10.0/24 out-interface=ether1 action=masquerade

[admin@MikroTik]> ip firewall nat add chain=srcnat

src-address=10.10.10.2-10.10.10.5 out-interface=ether1

action=masquerade

[admin@MikroTik]> ip firewall nat print

Flags: X – disabled, I – invalid, D – dynamic

0 chain=srcnat action=masquerade src-address=10.10.10.0/24

out-interface=ether1

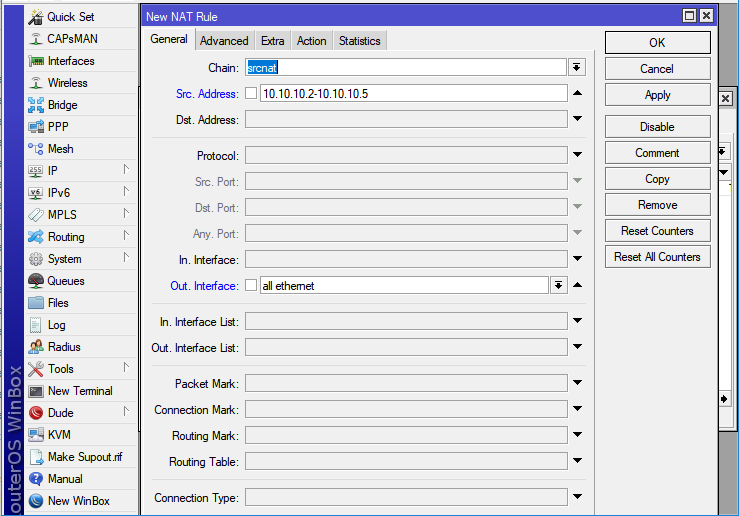
1 chain=srcnat action=masquerade src-address=10.10.10.2-10.10.10.5

out-interface=ether1

Setelah dilakukan pemeriksaan dengan perintah ip firewall nat print, maka terlihat ada dua baris konfigurasi NAT. Baris dengan index 0 menyatakan bahwa yang dapat mengakses internet adalah computer dengan ip address 10.10.10.0/24, sedangkan baris index 1 adalah 10.10.10.2 – 10.10.10.5.

Apa yang akan terjadi jika ternyata computer dengan ip address 10.10.10.6 mengakses internet? Router Mikrotik akan menganggap 10.10.10.6 termasuk dalam src-address=10.10.10.0/24 (index 0). Router Mikrotik akhirnya meloloskan computer 10.10.10.6 tersebut untuk mengakses internet.

Jika anda menggunakan WinBox, maka konfigurassi NAT ini dapat dilakukan melalui menu IP → firewall → Tab NAT, seperti gambar berikut :



*Gambar 3.4 Konfigurasi NAT menggunakan WinBox*

Untuk memilih *action=masquerade* pada WinBox, Anda dapat melakukannya dengan meng-klik tab *Action.*

**Masquerade untuk aplikasi tertentu**

Jika Anda menginginkan komputer user hanya mendapatkan layanan Internet tertentu (misalnya hanya memberikan akses browsing), maka Anda harus menambahkan aksi protocol dan destination port pada baris konfigurasi masquerade.

Anda harus mengetahui nomor-nomor port tujuan di server Internet untuk berbagai layanan (aplikasi). Misalnya destination port 80 untuk layanan browsing (HTTP), destination port 20 dan 21 untuk aplikasi FTP (File Transport Protcol), destination port 23 untuk layanan telnet atau pundestination port 22 untuk layanan remot SSH. Anda dapat melihat daftar destination port pada server-server Internet pada link berikut <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>

Pada sub bab ini saya akan memberikan contoh-contoh konfigurasi masquerade untuk layanan Internet yang umum di gunakan. Sedangkan untuk layanan lainnya, misalnya radio streaming, Anda dapat mencari nomor destination port-nya di situs-situs Internet.

Sebagai contoh, jika Anda menginginkan komputer 10.10.10.2 sampai 10.10.10.25

hanya mendapatkan layanan browsing (HTTP), maka konfigurasi yang harus Anda lakukan adalah sebagi berikut:

[admin@gateway] > ip firewall nat add chain=srcnat src-address=10.10.10.2-10.10.10.5 protocol=tcp dst-port=80 out-interface=ether1 action=masquerade

[admin@gateway] > ip firewall nat print

Flags: X – disabled, I – invalid, D – dynamic

0 chain=srcnat action=masquerade protocol=tcp src-address=10.10.10.2-10.10.10.5 out-interface=ether1 dst-port=80

Untuk website yang memiliki login username dan password, seperti Gmail, Yahoo, Mail, Facebook, biasanya menerapkan juga HTTPS, Anda harus menambahkan lagi opsi destination port 443, seperti berikut ini:

[admin@gateway] > ip firewall nat add chain=srcnat src-address=10.10.10.2-10.10.10.5 protocol=tcp dst-port=443 out-interface=ether1 action=masquerade

[admin@gateway] > ip firewall nat print

Flags: X – disabled, I – invalid, D – dynamic

0 chain=srcnat action=masquerade protocol=tcp src-address=10.10.10.2-10.10.10.5 out-interface=ether1 dst-port=80

1 chain=srcnat action=masquerade protocol=tcp src-address=10.10.10.2-10.10.10.5 out-interface=ether1 dst-port=443

Sebagai contoh lagi, jika Anda hanya menginginkan komputer 10.10.10.2 untuk mendapatkan layanan Yahoo Messenger, maka konfigurasi yang harus ditambahkan adalah sebagai berikut:

[admin@gateway] > ip firewall nat add chain=srcnat src-address=10.10.10.2 protocol=tcp dst-port=5050 out-interface=ether1 action=masquerade

Jika Anda menginginkan computer user dapat melakukan ping (protocol ICMP) ke situs-situs Internet, maka konfigurasi yang harus ditambahkan adalah sebagai berikut:

[admin@gateway] > ip firewall nat add chain=srcnat src-address=10.10.10.2 protocol=icmp out-interface=ether1 action=masquerade

Contoh-contoh konfigurasi masquerade tadi dapat Anda kembangkan sendiri. Sesuaikanlah dengan apa yang ingin anda berikan kepada komputer – komputer user. Jika ingin menggunakan WinBox, maka konfigurasi masquerade dengan opsi protocol dan dst-port dapat dilakukan melalui menu IP → Firewall → tab NAT. Untuk beberapa layanan yang menggunakan protocol yang sama (misalnya menggunakan protocol TCP), maka untuk mempersingkat konfigurasi, anda dapat membuat opsi dst-port=80,443,5050 seperti berikut :

[admin@MikroTik]> ip firewall nat add chain=srcnat

Src-address=10.10.10.2-10.10.10.5 protocol=tcp dat-port=80,443,5050 out-interface=ether1 action=masquerade

Sekali lagi saya mengingatkan untuk tidak menumpuk konfigurasi, perhatikan selalu baris-baris konfigurasi masquerade yang telah anda masukkan.

**Masquerade dengan fungsi waktu**

Router Mikrotik juga dapat membatasi akses layanan internet berdasarkan hari dan jam. Misalnya, anda ingin memberikan layanan HTTP/HTTPS pada komputer user hanya pada jam 08.00 – 16.00 untuk hari Senin, Selasa, Rabu, Kamis dan Jumat maka konfigurasi yang dapat digunakan adalah sebagai berikut.

[admin@gateway] > ip firewall net add chain=srcnat

src-address=10.10.10.2-10.10.10.5 protocol=tcp dst-port=80,443

time=08:00:00-16:00:00,mon,tue,wed,thu,fri

out-interface=ether1 action=masquerade

[admin@gateway] > ip firewall nat print

Flags : X – disabled, I – invalid, D – dynamic

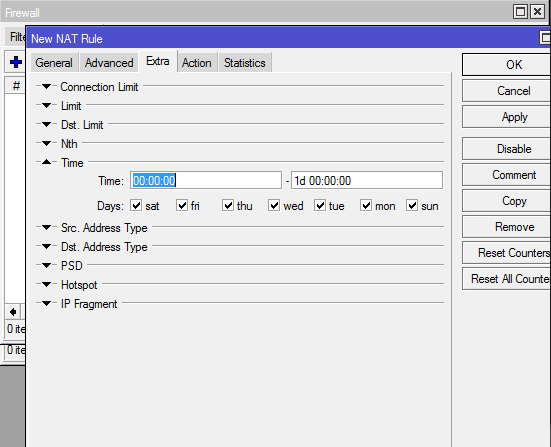
chain=srcnat action=masquerade protocol=tcp

src-address=10.10.10.2-10.10.10.5 out-interface=ether1

dst-port=80,443 time=8h-16h,mon,tue,wed,thu,fri

Anda harus memastikan bahwa konfigurasi waktu pada Router MikroTik sudah akurat. Konfigurasi ini sudah saya bahas pada Bab 2 dengan sub bab *Network Time Protokol (NTP).*

Jika menggunakan WinBox, Anda dapat melakukan penambahan opsi waktu ini melalui menu ***IP →Firewall→***tab ***NAT →*** tab ***Extra***,seperti gambar berikut.



*Gambar 3.6. Penambahan opsi waktu*

Filter

Fitur Filter pada firewall digunakan untuk menentukan apakah suatu paket data dapat masuk atau tidak ke dalam sistem router itu sendiri. Paket data yang akan ditangani fitur. Filter ini adalah paket data yang ditunjukan pada salah satu interface router. Anda harus membedakan dengan fungsi Nat yang Menangani paket yang akan melintasi router.sekaligus merubahIP Address pengirim dari paket data tersebut.

Meskipun demikian, fitur Filter inijuga dapat menangani paket data yang melintasi router dari jaringan local ke internet,sehingga fitur filter nantinya dapat dikolaborasikan dengan NAT.

Fitur filter pada router Mikrotik memiliki 3 chain, yaitu input,output dan forward.Pada buku ini,saya membagi pembahasan filter menjadidua bagiansaja, yaiutu penggunaan chain input dan chain forward.Sedangkan chain output yang berfungsi menanggani paket data yang berasal dari router itu sendiri tidak akan saya bahas.Saya tetap ingin membuat buku inisederhana dan merupakan pondasi jika Anda melanjutkan dengankonfigurasi-konfigurasi yang lebih rumit.

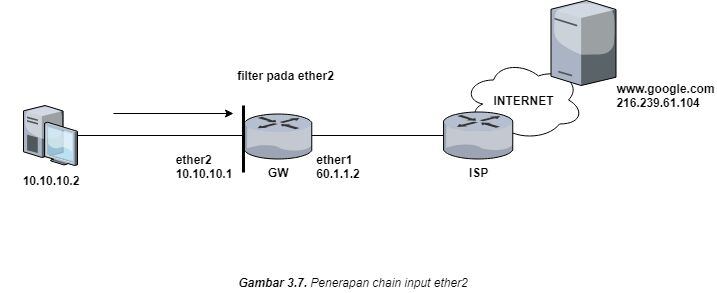
**Chain Input**

Chain input pada firewall akan menangani paket data yang ditujukan padainterface Router Mikrotik Anda. Paket data ini biasanya adalah paket data pada saat akan melakukan konfigurasi , misalnya pada saat anda memasukan IP Address 10.10.10.1 pada WinBox. Chain input ini berguna untuk membatasiakses konfigurasi terhadap Router Mikrotik.Anda tentunya tidak ingin orang lain melakukan percobaan konfigurasi terhadap Router Mikrotik Anda.

Pengunaan chain input dapat anda lihat pada ilustrasi gambar 3.7 , dimana ada sebuah paket data yang ditujukan kepada interface ether2.Karena melakukan perlindungan pada interface-interfacerouter, maka chain input ini dapat diterapkan pada dua interface Router Mikrotik Anda(padaether1 dan ether2).

Penerapan chain input pada interface ether1 berfungsi memberikan perlindungan terhadap akses yang mungkin terjadi dari internet.Sedangkan penerapannya pada ether2 memberikan perlindungan terhadap kemungkinan akses dari dalam jaringan Anda sendiri.Bukan tidak mungkin Anda mempunyai musuh dalam selimut yang selalu penasaran dengan Router Mikrotik Anda.

|  |
| --- |
| Src IP Address :10.10.10.2 |
| Dst IP Address :10.10.10.1 |
| DATA : WinBox |



Penerapan Filter dengan menggunakan *chain input* pada *ether 1,* ditujukan untuk membatasi akses terhadap port-port yang terbuka. Ini akan membatasi percobaan konfigurasi yang mungkin dilakukan dari Internet oleh orang-orang yang tidak bertaggung jawab . port yang terbuka secara default untuk keperluan konfigurasi pada Router Mikrotik adalah 22 (ssh), 23(telnet), 20&21(ftp), 80(WebFig), 8291(WinBox). Sehingga perintah yang dapat anda gunakan untuk menerapkan filter pada *ether 1* adalah sebagai berikut:

[admin@gateway] > ip firewall filter print

Flags: X – disabled, I – invalid, D – dynamic

0 chain-input action=drop protocol=top in-interface=ether1

dst-port=20,21,22,23,80,8291

Bila Anda menginginkan interface *ether 1* tidak dapat di *ping* dari Internet, maka Anda dapat menambahkan perintah berikut:

[admin@gateway] > ip firewall filter add chain=input in-interface=ether1 protocol=i cmp connection-state=establishedaction=accept

[admin@gateway] > ip firewall filter add chain=input in-interface=ether1 protocol=i cmp actiom=drop

Jika digabungkan dengan konfigurasi filter sebelumnya, maka akan terlihat seperti berikut:

[admin@gateway] > ip firewall filter print

Flags: X – disabled, I – invalid, D – dynamic

0 chain-input action=drop protocol=top in-interface=ether1dst-port=20,21,22,23,80,8291

1 chain=input action=accept connection-state=established protocol=icmp in-interface=ether1

2 chain=input action=drop protocol=icmp in-interface=ether1

Baris dengan index 1,merupakan konfigurasi dengan penambahan *connection-state=established* yang berfungsi tetap mengizinkan paket *ping* masuk ke interface *ether 1* jika paket tersebut semula memang berasal dari Router Mikrotik itu sendiri. Tentunya anda tetap menginginkan Router Mikrotik dapat melakukan *ping*  kepada orang lain, namun orang lain tidak dapat melakukan *ping* kepada Router Mikritik anda.

Penerapan filter dengan *chain input* pada interface *ether 1* akan menimbulkan Polemik. Anda ingin membatasi orang lain untuk mengakses Router Mikrotik dari Internet. Namun bagaimana jika niatnya tiba-tiba anda ingin mengakses Router Mikrotik untuk melakukan konfigurasi dan maintenance dari Internet? Anda bias saja sedang berada di luar kota namun tiba-tiba harus melakukankonfigurasi pada router Anda yang ada di kantor.

Jika hal seperti diatas terjadi, maka anda harus mengizinkan paket data tertentu untuk masuk ke interface ether . Misalnya jika anda ingin mengizinkan computer dengan IP address 64.110.100.2 untuk melakukan konfigurasi dengan menggunakan WinBox(dst-port 8291), maka konfigurasi yang harus ditambahkan adalah perintah dengan action=accept seperti berikut :

[admin@gateway] > ip firewall filter add chain=input

In-interface=ether1 protocol=tcp dst-port=8291

Src-address=64.110.100.2 action=accept

Bola terdapat rule, maka Router Mikrotik akan mengeksekusi baris-baris konfigurasi tersebut dengan prinsip “top to buttom”. Sehingga urutan dari konfigurasi sangat berpengaruh terhadap tujuan akhir yang diinginkan. Sebagai contoh, berikut hasil konfigurasi yang telah anda lakukan sebelumnya. Anda bermaksud memberikan izin computer 64.110.100.2 untuk dapat melakukan konfigurasi melalui WinBox dari Internet.

[admin@gateway] > ip firewall filter print

Flags : X – disabeled, I – invalid, D – dynamic

0 chain=input action=drop protocol=top in-interface=ether1

Dst-port=20,21,22,23,80,829

Konfigurasi di atas akan tetap tidak memberikan akses konfigurasi bagi computer 64.110.100.2. Bagaimana ini bias terjadi? Ingat prinsip “top to buttom” yang akan digunakan Router Mikrotik pada saat akan meng-eksekusi baris-baris konfigurasi firewall filter.

Pada saat computer 64.110.100.2 melakukan akses dengan menggunakan WinBox terhadap ether1, maka Router Mikrotik akan menggunakan baris dengan index 0 untuk menangani paket data tersebut. Pada baris 0 tidak diacantumkan src-address. Sehingga Router Mikrotik akan melakukan action drop (membuang paket data) jika ada sembarang computer (termasuk 64.110.100.2) yang melakukan akses konfigurasi dengan menggunakan WinBox. Ini menyebabkan Router Mikrotik tidak lagi menggunakan baris konfigurasi dengan nomor index 3, padahal baris tersebut seharusnya akan mengizinkan akses konfigurasi dari computer 64.110.100.2. Logika berfikirnya adalah *”bagaimana mugkin anda sudah memblok semua IP Address di Internet sedangkan anda masih ingin memberikan akses ke seluruh computer lagi”.*

Untuk membuat konfigurasi yang dimaksud dapat berjalan sesuai scenario, maka anda harus merubah susunan baris-baris filter tersebut. Anda harus menempatkan baris yang mengizinkan computer 64.110.100.2 melakukan akses WinBox (src-address=64.110.100.2 action=accept) menjadi baris pertama, diatas baris yang melakukan blokir terhadap semua IP Address di Internet. Anda dapat melakukan blokir dengan perintah sebagai berikut :

[admin@MikroTik]> ip firewall filter move 3 0

Sebelum melakukan perpindahan baris konfigurasi, anda melihat susunan terlebih dahulu dengan menggunakan perintah ip firewall filter print. Sedangkan untuk sisi interface ether2 yang dihubungkan dengan jaringan local, anda juga dapat menerapkan filtering dengan chain input. Contoh berikut adalah adalah konfigurasi yang membatasi akses konfigurasi dari keseluruhan computer yang ada dalam jaringan 10.10.10.0/24, namun memberikan akses konfigurasi (baik SSH, telnet, WinBox maupun ping) dari computer 10.10.10.4 yang diskenariokan sebagai computer yang sering digunakan oleh administrator jaringan.

[admin@MikroTik]> ip firewall filter add chain=input

In-interface=ether2 src-address=10.10.10.4 action=accept

[admin@MikroTik]> ip firewall filter add chain=input

In-interface=ether2 protocol=icmp connection-state=estabilished action=accept

[admin@MikroTik]> ip firewall filter add chain=input

In-interface=ether2 protocol=icmp action=drop

[admin@gateway] > ip firewall filter add chain=input

In-interfae=ether2 protocol=tcp dst-port=20,21,22,23,80,8291

action=drop

[admin@gateway] > ip firewall filter print

Flags: X - disabled, I - invalid, D - dynamic

1. chain=input action=accept protocol=tcp src=address=64.110.100.2

in-interface=ether1 dst-port=8291

1. chain=input action=drop protocol=tcp in-interface=ether1

dst-port=20,21,22,23,80,8291

1. chain=input action=accept connection-state=established

protocol=icmp in-interface=ether1

1. chain=input action=drop protocol=icmp in-interface=ether1
2. chain=input action=accept src-address=10.10.10.4

in-interface=ether2

1. chain=input action=accept connection-state =established

protocol=icmp in-interface=ether2

1. chain=input action=drop protocol=icmp in-interface=ether2
2. chain=input action=drop protocol=tcp in-interface=ether2

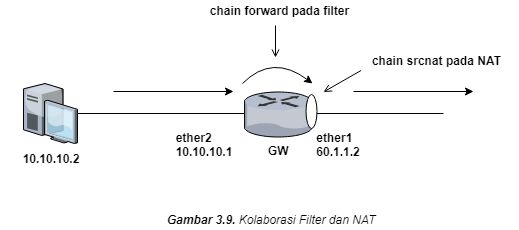
dst-port=20,21,22,23,80,8291

Bila Anda menggunakan WinBox, maka konfigurasi firewall untuk Filter dapat diakses melalui menu IP🡺Firewall🡺tab Filter.

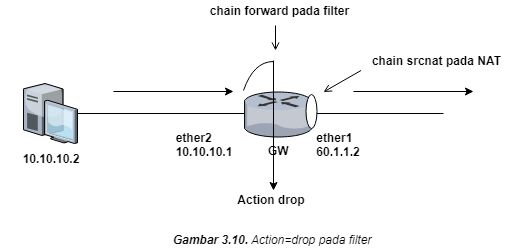
Untuk menentukan *action* jika menggunakan WinBox, Anda dapat melakukannya melalui tab *Action*. Sedangkan jika ingin mengubah susunan baris konfigurasi firewall pada WinBox, Anda dapat melakukannya dengan cara *drag and drop*.

**Chain Forward**

*Chain forward* pada Filter Router Mikrotik digunakan untuk menangani paket data yang akan melintas router. Sepintas akan terlihat sama dengan NAT yang sudah kita bahas sebelumnya. *Chain forward* memang akan menanganni paket data yang melintas router, baik paket data dari jaringan local yang ingin ke Internet maupun sebaliknya, sama dengan yang dilakukan oleh NAT. Namun perbedaan keduanya adalah jika *chain srcnat* pada NAT menangani paket data dengan melakukan perubahan IP Address pengirim. Untuk mempermudah memahami keduanya Anda dapat melihat gambar berikut :



Pada gambar di atas, terlihat akses Internet dari computer 10.10.10.2 akan diterima di *ether2.* Router Mikrotik akan menggunakan Filter dengan *chain* *forward* terlebih dahulu untuk memerikas paket data tersebut. Kemudian paket data diserahkan ke NAT yang akan mengubah IP Address pengirim dari paket data tersebut. Sehingga akan terlihat bahwa *Chain forward* pada Filter memegang kendali terlebih dahulu sebelum *chain srcnat* pada NAT. ini mengakibatkan konfigurasi *action-masquerade* pada NAT tidak akan berfungsi jika *action=drop* telah dijalankan di *chain forward* pada Filter, seperti terlihan pada gambar berikut:



Contoh konfigurasi berikut memperlihatkan bahwa NAT dengan *chain=srcnat* telah memberikan akses Internet yang penuh pada semua komputer di jaringan 10.10.10.0/24. Namun konfigurasi pada Filter dengan *chain=forward* hanya mengizinkan akses Internet pada komputer 10.10.10.2, 10.10.10.3, 10.10.10.4 dan 10.10.10.5.

Konfigurasi masquerade yang menginzinkan semua komputer dalam jaringan 10.10.10.10.5 untuk mengakses Internet, seperti terlihat berikut :

[admin@gateway] > ip firewall nat print

Flags: X – disabled, I – invalid, D – dynamic

0 chain=srcnat action=masquerade src-address=10.10.10.0/24 out-interface=ether1

Kemudian dilakukan penambahan konfigurasi Filter dengan *chain forward* yang hanya mengizinkan komputer 10.10.10.2 sampai 10.10.10.5 untuk mengakses Internet, seperti berikut :

[admin@gateway] > ip firewall filter add chain=forward src-address=10.10.10.2-10.10.10.5 in-interface=ether2 action=accept

[admin@gateway] > ip firewall filter add chain=forward src-address=10.10.10.0/24 in-interface=ether2 action=drop

Sehingga hasil konfigurasinya dapat anda lihat seperti berikut :

[admin@gateway] > ip firewall filter print

Flags: X – disabled, I – invalid, D – dynamic

0 chain=forward action=accept src-address=10.10.10.2-10.10.10.5 in-interface=ether2

1 chain=forward action=drop src-address=10.10.10.0/24 in-interface=ether2

Yang menjadi pertanyaan selanjutnya, apakah anda harus menggunakan chain forward bila sudah ada konfigurasi masquerade pada NAT? Bukankah pemblokiran akses internet seperti yang telah dijelaskan di sub bab Masquerade terdahulu sudah dirasa cukup? Jika anda sudah merasa cukup dengan manajemen jaringan dengan menggunakan NAT, makan penggunaan chain forward ini tidak perlu anda terapkan. Secara default chain forward sudah berjalan dan akan memberikan akses penuh ke internet bagi semua komputer user. Namun jika anda merasa harus meningkatkan efektifitas manajemen jaringan dan konfigurasi maquerade pada NAT tidak mampu lagi melakukannya, mungkin anda harus mempertimbangkan untuk menggunakan chain forward pada Filter Router Mikrotik.

**Chain Forward dan content**

Anda dapat menggunakan chain forward untuk memblokir akses internet terhadap situs tertentu maupun aktifitas user yang ingin mendownload jenis-jenis file tertentu. Untuk melakukannya anda harus menggunakan option content yang ada pada fitur Firewall Filter. Contoh berikut memperlihatkan konfigurasi yang akan memblokir akses internet ke situs [www.playboy.com](http://www.playboy.com) dan aktifitas download file mp3.

[admin@gateway] > ip firewall filter add chain=forward

src-address=10.10.10.0/24 content=www.playboy.com action=drop

[admin@gateway] > ip firewall filter add chain=forward

src-address=10.10.10.0/24 content=.mp3 action=drop

[admin@gateway] > ip firewall filter print

Flags : X – disabled, I –invalid, D – dynamic

0 chain=forward action=drop src-address=10.10.10.0/24 content=www.playboy.com

1 chain=forward action=drop src-address=10.10.10.0/24 conten=.mp3

Dengan mengunakan opsi content= [www.playboy.com](http://www.playboy.com), bila ada komputer user yang memasukkan kata [www.playboy](http://www.playboy) .com pada mesin pencari (Search Engine), maka Search Engine tidak akan memberikan hasil apapun.

Untuk menggunakan opsi content dengan menggunakan WinBox, Anda dapat melakukannya melalui menu IP -> Firewall ->Filter -> tab Advanced.

Ingatlah selalu bahwa urutan dari baris-baris konfigurasi Firewall sangat menentukan efektif tidaknya konfigurasi akhir yang anda inginkan. Jangan sampai anda sudah melakukan pemblokiran seperti diatas, namun anda menempatkannya di bawah baris konfigurasi yang ternyata memberikan akses internet penuh kepada komputer user.

**Action=drop vs action=reject**

Pada konfigurasi-konfigurasi sebelumnya, opsi action yang digunakan untuk memblokir adalah drop. Anda dapat melihat contoh berikut ini yang tidak memberikan akses internet kepada komputer user 10.10.10.6 s/d 10.10.10.254 dengan menggunakan chain=forward dan action=drop.

[admin@gateway] > ip firwall filter print

Flags: x – disabled, I = invalid, D = dynamic

0 chain=forward action=accept src-address=10.10.10.2-10.10.10.3

1 chain=forward action=drop src-address=10.10.10.0/24

Anda dapat saja mengganti *action=drop* menjadi *action=reject* yang sama-sama juga akan memblokir akses Internet bagi komputer user 10.10.10.6 s/d 10.10.10.254.

Berikut perbedaan antara *drop* dan *reject*. Jika *drop* yang anda pilih maka paket data yang berasal dari computer-komputer tersebut akan dibuang oleh router (drop). Sedangkan jika anda memilih *reject,* maka paket data akan dibuang oleh router namun router akan memberikan pemberitahuan kepada computer user. Pemberitahuan ini menggunakan protocol ICMP (*Internet Control Message Protocol*).

Contoh perintah yang dapat anda gunakan adalah sebagai berikut :

[admin@gateway] > ip firewall filter add chain=forward

src-address=10.10.10.2-10.10.10.5 action=accept

[admin@gateway] > ip firewall filter add chain=forward

src-address=10.10.10.0/24 action=reject

reject-with=icmp-host-unreachable

[admin@gateway] > ip firewall filter print

Flags: X – disabled, I – invalid, D – dynamic

0 chain=forward action=accept src=address=10.10.10.2-10.10.10.5

1 chain=forward action=reject reject-with=icmp-host-unreachable

src-address=10.10.10.0/24

Pada saat komputer 10.10.10.6 s/d 10.10.10.254 melakukan ping ke Internet, pesan ICMP yang akan didapatkan oleh komputer tersebut dapat Anda lihat adalah

***”Reply from 10.10.10.1: Destination net unreachable.”***

***”Reply from 10.10.10.1: Destination net unreachable.”***

***”Reply from 10.10.10.1: Destination net unreachable.”***

***”Reply from 10.10.10.1: Destination net unreachable.”***

Kembali lagi, jika *action=drop* yang Anda gunakan, maka yang terlihat pada komputer user pada saat melakukan ping adalah *”request time out”.*

**Address List**

Router Mikrotik menyediakan fitur Address List untuk merujuk IP Address tertentu dengan sebutan nama. Fitur ini dapat digunakan untuk keperluan deklarasi IP Address maupun untuk kepentingan logging (pencatatan aktifitas jaringan)

Penggunaan deklarasi IP Address menjadi sebuah nama akan membuat Anda tidak terlalu repot mengelola jaringan jika suatu saat terjadi perubahan IP Address. Sebagai contoh, anda ingin memberikan akses yang seluas-luasnya bagi komputer Administrator dengan IP Address 10.10.10.4. Namun tiba-tiba sang Administrator tidak ingin lagi menggunakan IP Address tersebut dan ingin menggunakan komputer dengan IP Address 10.10.10.3. Ini akan mengakibatkan anda harus merubah seluruh konfogurasi yang sudah dibuat pada Filter maupun NAT. Dengan menggunakan Address List, anda hanya cukup merubah deklarasi IP Address bahwa komputer Administrator sudah berpindah ke IP Address 10.10.10.3.

Berikut contoh penggunaan Address List untuk mendeklarasikan IP Address dalam jaringan, termasuk komputer milik Administrator.

[admin@gateway] > **ip firewall address-list add address=10.10.10.0/24 list=”jaringan lokal”**

[admin@gateway] > **ip firewall address-list add address=10.10.10.4 list=”pc admin”**

[admin@gateway] > **ip firewall address-list print**

Flags: X – disabled, D – dynamic

# LIST ADDRESS

0 jaringan lokal 10.10.10.0/24

1 pc admin 10.10.10.4

Bila anda ingin menggunakan spasi pada baris konfigurasi, gunakanlah tanda “, seperti opsi list=”jaringan lokal” pada baris konfigurasi di atas.

Selanjutnya jika anda ingin melakukan konfigurasi pada bagian firewall, anda tidak perlu lagi menuliskan IP Address 10.10.10.0/24 ataupun 10.10.10.4. Contoh berikut memperlihatkan penggunaan Address List pada konfigurasi NAT.

[admin@gateway] > **ip firewall nat add chain=srcnat out-interface=ether1 src=address-list=”pc admin” action=masquerade**

[admin@gateway] > **ip firewall nat add chain=srcnat out-interface=ether1 src=address-list=”jaringan lokal” protocol=top dst-port=80,443 action=masquerade**

[admin@gateway] > **ip firewall nat print**

Flags: X - disabled, I - invalid, D - dynamic

1. chain=srcnat action=masquerade src-address-list=pc admin

out-interface=ether1

1. chain=srcnat action=masquerade protocol=tcp

src-address-list=jaringan lokal out-interface=ether1

dst-port=80,443

Konfigurasi di atas bermaksud memberikan akses Internet yang penuh bagi komputer Administrator (ditandai dengan *src-address-list=”pc admin”* ). Namun Konfigurasi diatas, hanya memberikan akses browsing (HTTP/HTTPS) pada komputer-komputer lain (ditandai dengan *src-address-list=”jaringan lokal”*). jika suatu saat komputer Administrator berpindah lagi, maka perubahan konfigurasi hanya perlu dilakukan pada Address List, tidak perlu Anda lakukan pada firewall.

Contoh berikut memperlihatkan perubahan IP Address pada deklarasi Address List.

[admin@gateway] > **ip firewall address-list print**

Flags: X - disabled, D - dynamic

# LIST ADDRESS

0 jaringan lokal 10.10.10.0/24

1. Pc admin 10.10.10.4

[admin@gateway] > ip firewall address-list set 1 address=10.10.10.3

[admin@gateway] > **ip firewall address-list print**

Flags: X - disabled, D - dynamic

# LIST ADDRESS

0 jaringan lokal 10.10.10.0/24

1 admin 10.10.10.3

Untuk mengkonfigurasi Address List melalui WinBox, Anda dapat melakukannya melalui menu ***IP->Firewall->***tab ***Address Lists.***

Langkah selanjutnya, anda dapat mengelola IP Address yang sudah tersimpan di Address List dengan menggunakan konfigurasi Firewall lainnya. Misalnya anda ingin memblokir akses dari computer-komputer yang sudah tercatat di Address List tadi. Perintah yang dapat digunakan adalah sebagai berikut :

[admin@MikroTik]> ip firewall filter add chain=input

src-address-list=”ping ilegal” action=dropi

[admin@MikroTik]> ip firewall filter add chain=input

src-address-list=”akses ilegal” action=drop

[admin@MikroTik]> ip firewall filter print

Flags: X – disabled, I – invalid, D – dynamic

0 chain=input action=add-src-to-address-list protocol=icmp

address-list=ping ilegal address-list-timeout=0s

in-interface=ether2

1 chain=input action=add-src-to-address-list protocol=tcp

address-list=akses ilegal address-list-timeout=0s

in-interface=ether2 dst-port=2223,8291

chain=input action=drop src-address-list=ping ilegal

3 chain=input action=drop src-address-list=akses ilegal

Akses juga dapat mengkolaborasikan antara penggunaan Address List dengan Network Address Translation pada Firewall.