FIREWALL

MENGENAL *FIREWALL* MIKROTIK

Firewall adalah sistem keamanan jaringan yang digunakan untuk melindungi jaringan dari akses yang tidak diizinkan serta mengendalikan lalu lintas jaringan berdasarkan aturan keamanan yang telah ditentukan. Fungsi dari *Firewall* secara umum digunakan untuk memeriksa dan menentukan aliran paket data yang masuk dan keluar dalam jaringan. Mengontrol dan mengawasi aliran paket data dijaringan. Mengawasi paket data yang diizinkan masuk dari jaringan public ke jaringan local.

Untuk dapat mempelajari *Firewall* dengan baik, maka kita seharusnya sudah memiliki pengetahuan mengenai IP packet yang meliputi informasi mengenai IP address pengirim (*source address*), IP address penerima (*destination address*), port pengirim dan port tujuan. Selain itu kita juga sebaiknya sudah mengetahui jenis *protocol* yang digunakan dalam aplikasi jaringan internet seperti *protocol* tcp, UDP, ICMP.

Firewall di Router mikrotik dapat melakukan filtering akses (*filter rule*), *forwarding packet* (NAT) serta menandai paket yang masuk dan keluar router (*mangle*). Agar fitur *Firewall* ini berjalan dengan baik maka diperlukan aturan (rule) yang tepat.

Parameter utama dalam membuat rule *Firewall* ini diatur dalam *chain*. Parameter *chain* digunakan untuk menentukan jenis lalu lintas data yang akan diatur dalam *Firewall*. Parameter chain pada *Firewall* filter rule, NAT dan Mangel memiliki pilihan chain yang berbeda. Pengisian parameter chain mengacu pada traffic flow routerOS. Setiap versi RouterOS memiliki skema traffic flow yang berbeda. Sebelum kita melakukan filter paket data yang masuk dan keluar di router kita harus mengenali terlebih dahulu jenis paket data yang akan kita atur menggunakan *Firewall*. Chain dianalogikan sebagai tempat untuk mencegat sebuah traffic data dan melakukan filtering sesuai kebutuhan.

FILTER RULE

Filter rule adalah *Firewall* yang digunakan untuk melakukan kebijakan hak akses sebuah traffic yang ada dalam jaringan. Setiap *Firewall* filer rule yang disusun diorganisir dalam bentuk *chain* (rantai).

Dalam menu *Firewall-filter rule* ada 3 chain yaitu *input, output, forward*. Setiap aturan rule chain yang dibuat akan dibaca oleh router dari rule paling atas ke bawah.

Chain input, digunakan untuk mengelola paket yang masuk menuju router melalui salah satu interface router dan alamat IP yang dimiliki router. Jenis traffic rule ini bisa berasal dari jaringan public maupun jaringan local. Contoh akses ke router menggunakan winbox,ssh,telnet dari jaringan public dan local. Kita tidak menginginkan adanya akses yang tidak diizinkan kedalam router.

Penerapan chain input dalam jaringan digunakan untuk membatasi akses terhadap beberapa port router yang terbuka baik dari dalam maupun dari luar. Secara default port yang terbuka di router mikrotik seperti ssh 22, telnet 23, ftp 21, winbox 8291, webfig 80.

Chain forward, digunakan untuk mengelola paket yang masuk ke router dan kemudian diteruskan ke tujuan dengan cara melewati router. Misalnya traffic dari jaringan public ke jaringan local. Contohnya ketika melakukan browsing internet maka *Firewall* filter akan

mengelola paket dengan chain forward.

Di router sesuai dengan *filter rule* yang ditetapkan, maka paket akan diteruskaN NAT untuk dilakukan perubahan IP local menjadi IP public dan selanjunya diteruskan ke internet. Selain itu kita bisa menggunakan *chain forward* untuk melakukan filter terhadap konten website dan ekstensi file yang diakses client.

Chain output, digunakan untuk mengelola traffic yang keluar dari router ke alamat tujuan. Jadi traffic berasal dari dalam router ke *destination network*. Misalnya adalah akses ping, Penerapan chain output salah satunya adalah dengan pengaturan jika ada percobaan login ke router salah sebanyak beberapa kali maka router akan melakukan blokir terhadap IP address tersebut. Konfigurasi ini selanjutnya akan dibahas di studi kasus.

NAT
NAT *(Network Address translation*) adalah salah satu konfigurasi yang dilakukan untuk menghubungkan jaringan local yang memiliki IP Private ke internet.

Sebelumnya kita sudah menjelaskan bahwa jaringan internet berkomunikasi dengan IP *Public* yang teregistrasi dan sudah terdaftar oleh ISP. Tetapi tidak mungkin rasanya jika di jaringan local semua host menggunakan *IP public* untuk berkomunikasi karena IPv4 memiliki jumlah yang terbatas. Untuk itu agar client dengan IP Private bisa akses intenet maka digunakan Teknik NAT Masquerade.

Pada *Firewall* Nat ada 2 chain yang digunakan yaitu **srcnat** (*source nat*) dan **dstnat** (*destination nat*).
Srcnat digunakan untuk mengubah paket asal (*source*) address yang berasal dari jaringan yang akan diubah yaitu jaringan local/private. Dengan *srcnat* maka IP private akan disembunyikan dan digantikan dengan IP Public (masquerade).

Dstnat digunakan untuk mengubah destination address pada sebuah paket data. Biasa digunakan untuk membuat host dalam jaringan lokal dapat diakses dari luar jaringan (internet) dengan cara NAT akan mengganti alamat IP tujuan paket dengan alamat IP lokal.

Filter rule - Membatasi akses sebuah IP ke router
Konfigurasi agar yang bisa akses dan ping ke router 1 hanya IP 192.168.10.2

/Ip firewall filter add chain=input src-address=192.168.10.2 action=accept
/Ip firewall filter add chain=input action=drop

Hasilnya adalah PC 1 192.168.10.2 bisa melakukan ping ke router dan IP PC2 192.168.10.2 tidak bisa ping ke router.

Jika kita melihat filter rule print, maka ada 2 rule yang dibuat sesuai urutan pertama dengan index 0 adalah mengizinkan IP 192.168.10.2 untuk akses ke router, kemudian rule kedua dengan index 1 artinya melakukan drop paket kepada semua input IP yang masuk ke router. Jadi penerapan metode ini disebut dengan metode *accept few, drop any*.
Filter yang kita buat sebelumnya hanya melakukan drop ping, namun jika dicoba PC 2 192.168.10.3 bisa melakukan akses ke winbox.

Filter rule - Membatasi akses ke Port router
Untuk melakukan filter akses ke winbox ada beberapa cara, kali ini kita gunakan filter rulenya saja. Sama seperti kondisi filter sebelumnya hanya di rule drop tambahkan port winbox = 8291 dan definisikan interface yang digunakan.

/ip firewall add chain=input src-address=192.168.10.2 action=accept
/ip firewall add chain=input protocl=tcp dst-port=8291 in-interface=ether2 action=drop

Hasilnya adalah client PC2 tidak bisa login ke winbox.

Filter rule - Membatasi akses semua client ke router
Kita ingin agar router kita tidak bisa di ping dari client intenet , maka penerapan rule filternya adalah:

/ip Firewall filter add chain=input in-interface=ether1 protocol=icmp action=drop

Ada kalanya kita ingin melakukan remote router dari intenet, namun berdasarkan rule diatas kita sudah melakukan blokir akses kesemua port router sehingga tidak memungkinkan untuk melakukan akses ke router dari luar. Untuk kasus seperti ini bisa kita atasi dengan menambakan alamat IP yang diizinkan untuk melakukan akses ke router dari internet. Rule yang kita gunakan adalah:

/ip firewall filter add chain=input action=accept protocol=tcp srcaddress=alamat_ip_public in-interface=ether1

Filter Rule – Address list filter
Ada kalanya kita ingin melakukan filter terhadap sekelompok IP address di dalam jaringan. Mikrotik mempunyai fitur address list untuk mengelompokkan IP address tertentu berdasarkan metworknya kedalam system penamaan yang kita inginkan. Address list digunakan untuk melakukan filter terhadap group IP dengan 1 *Firewall* rule.

Addres List juga merupakan hasil dari rule *Firewall* dengan action=add to address list. Untuk satu address list bisa memuat subnet, range IP, atau 1 host IP address.
Buatlah rule *Firewall* yang akan memasukkan setiap IP address yang melakukan ping ke router ke dalam table address list.

/ip firewall filter add chain=input protocol=icmp action=add-src-to-address-list addres=list=tukangping

Kemudian cobalah untuk melakukan ping dari pc client ke IP router. Terlihat secara otomatis IP address yang melakukan ping akan masuk ke table address list dengan kelompok nama=tukang-ping.

Kemudian buat rule yang memblokir akses tukang ping ke router.

/ip Firewall filter add chain=input src-address-list=tukang-ping action=drop

Maka hasilnya semua IP yang ada di table address list tidak bisa lagi ping ke router.

Filter akses ke website dengan filter rule

Administrator ingin agar client dijaringannya tidak dapat melakukan akses ke website tertentu, missal ke situs porno,situs judi dan lain lainnya. Untuk melakukan filter tersebut dapat dilakukan salah satunya dengan filter rule *Firewall*.

Langkah 1. Mengetahui IP server domain yang akan diblok, bisa dengan menggunakan ping domain.

Langkah 2. Tambahkan filter rule di *Firewall*

/ip Firewall filter add chain=forward dst-address=159.148.147.196 action=drop

Terlihat di client browser tidak dapat menampilkan halaman web mikrotik.com.

Permasalah yang muncul dari menggunakan filter ini adalah ada beberapa website besar seperti facebook.com, youtube,com dll yang memiliki puluhan alamat IP server yang berbeda. Tentunya administrator akan kesulitan untuk melakukan filter seperti ini. Cara yang digunakan jika IP servernya banyak bisa menggunakan Teknik *add-to-address-list*. Kita mengelompokkan IP server youtube.com di address list yang akan terdata secara otomatis di table address list kemudian lakukan drop dengan parameter address list.