J-SISKO TECH (Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD)
Vol.4. No.2, Juli 2021, pp. 173-179
E-ISSN: 2615-5133

Pemanfaatan Firewall Pada Jaringan Mengunankan Mikrotik RB951Ui – 2HnD

Nama MahasiEpi Rahmat Putra Gulo, Devri Suherdi, Syarifah Fadillah Rezky
Teknik Informatika , Politeknik Ganesha Medan
Sistem Informasi , STMIK Triguna Dharma
Sistem Informasi, STMIK Triguna Dharma

Article Info
Article history:
Received Jun 06th, 2021
Revised Jul 23th, 2021
Accepted Jul 30th, 2021

Keyword:
Firewall
Packet Filtering
Router Microtik

ABSTRACT
Pemanfaatan firewall pada jaringan sangatlah diperlukan, apalagi yang terhubung dengan jaringan internet, sangat rentan sekali terhadap penyusupan, pencurian data serta penyalahgunaan informasi oleh orang yang tidak bertanggung jawab.
Router Mikrotik merupakan perangkat yang memiliki fitur firewall yang dapat dimanfaatkan pada jaringan. Sehingga nantinya setiap kegiatan pertukaran paket data yang terjadi harus melewati firewall.

Corresponding Author:
Nama :Devri Suherdi
Program Studi : Sistem Informasi
STMIK Triguna Dharma
Email: devrisuherdi10@gmail.com

1. PENDAHULUAN

Sebuah jaringan yang baik haruslah mempunyai tingkat firewall yang baik. **Firewall** itu sendiri merupakan sistem atau 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 luar.

Mikrotik merupakan perangkat keras yang memiliki fitur sangat lengkap. Penggunaan mikrotik pada sebuah jaringan sangatlah baik, karena mikrotik mempunyai fitur firewall sehingga penyedia jaringan dapat memanfaatkan fitur tersebut pada jaringan. Berdasarkan uraian di atas, penulis tertarik untuk mengangkat judul penelitian "Pemanfaatan Firewall Pada Jaringan Menggunakan Mikrotik RB951Ui-2HnD".

2. METODE PENELITIAN

Metode penelitian adalah teknik atau cara mencari, memperoleh, mengumpulkan, atau mencatat data yang dapat digunakan untuk menyusun karya ilmiah kemudian menganalisa faktor-faktor yang berhubungan dengan pokok-pokok permasalahan sehingga didapat kebenaran atas data yang diperoleh (Sintasuhan, 2010).

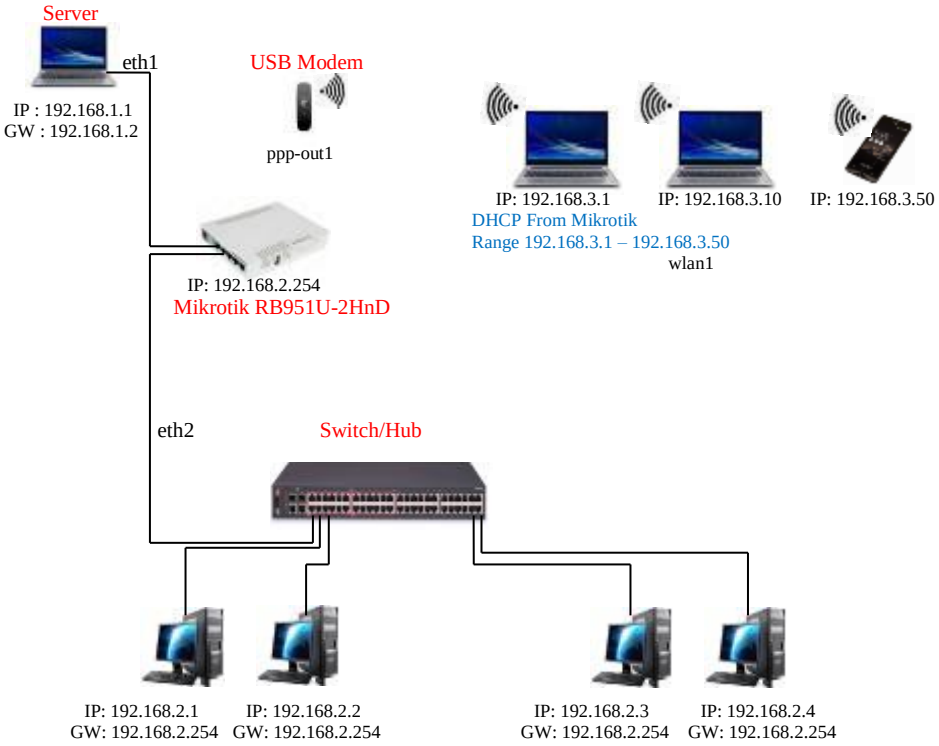
Pelaksanaan penelitian ini direncanakan berlangsung mulai bulan Januari 2016 sampai Februari 2016. Penelitian ini dilaksanakan di Kampus Politeknik Ganesha Medan.

Peralatan atau perangkat yang digunakan pada penelitian ini digolongkan menjadi 2 jenis, yaitu perangkat keras (*Hardware*) dan perangkat lunak (*Software*)

1. **Perangkat Keras**
   Router Board Mikrotik RB951Ui-2HnD
2. **Perangkat Lunak**
   Aplikasi Winbox

3. ANALISA DAN HASIL

1.1 Topologi Jaringan Yang Dibangun



Gambar 3.1 Topologi Jaringan

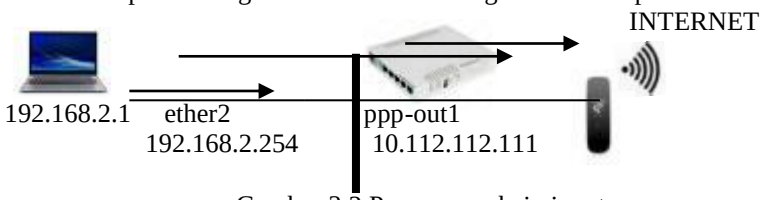
1.2 Konfigurasi Firewall Mikrotik

Konfigurasi Firewall Mikrotik

A. Firewall Filter Rules

a. Chain Input

Chain input pada firewall akan menangani paket data yang ditujukan pada interface Router Mikrotik. Chain input ini berguna untuk akses konfigurasi terhadap Router Mikrotik.



Gambar 3.2 Penerapan chain input

Penerapan chain input pada interface ppp-out1 berfungsi memberi perlindungan akses yang mungkin terjadi dari internet, yaitu membatasi akses terhadap port-port yang terbuka, sehingga membatasi percobaan konfigurasi yang mungkin dilakukan dari internet oleh orang yang tidak bertanggung jawab. Berikut adalah langkah-langkahnya:

1. Buka menu New Terminal →ketikkan perintah dibawah ini

   [admin@MikroTik] > ip firewall filter add chain=input in-interface=ppp-out1 protocol=tcp dst-port=20,21,22,23,80,8291 action=drop

   Agar interface ppp-out1 tidak dapat di ping dari internet

   [admin@MikroTik] > ip firewall filter add chain=input in-interface=ppp-out1 protocol=icmp connection-state=established action=accpet
   [admin@MikroTik] > ip firewall filter print

2. Selanjutnya pada interface ether2 terapkan juga filtering dengan chain input. Disini membatasi konfigurasi seluruh komputer yang ada di dalam jaringan 192.168.2.0/24, namun memberi akses terhadap 192.168.2.27.

   [admin@MikroTik] > ip firewall filter add chain=input in-interface=ether2 src-address=192.168.2.27 action=accpet
   [admin@MikroTik] > ip firewall filter add chain=input in-interface=ether2 protocol=tcp dst-port=20,21,22,23,80,8291 action=drop

b. Chain Forward

Digunakan untuk menangani paket data yang akan melintasi router. Berikut beberapa penggunaan chain forward :

1. Perintah yang digunakan untuk memblokir akses internet terhadap situs www.facebook.com
   New Terminal →ketikkan perintah dibawah ini
   [admin@MikroTik] > ip firewall filter add chain=forward src-address=192.168.2.0/24 content=www.facebook.com action=drop
   Perintah untuk memblokir aktifitas download file .mp3
   [admin@MikroTik] > ip firewall add chain=forward src-address=192.168.2.0/24 content=.mp3 action=drop

2. Membloklir akses internet terhadap komputer user kecuali 192.168.2.10 s/d 192.168.2.20 menggunakan chain=forward dan action=reject yang nantinya router akan memberikan pemberitahuan kepada komputer user melalui protokol ICMP (*Internet Control Message Protokol*).
   [admin@MikroTik] > ip firewall filter add chain=forward src-address=192.168.2.10-192.168.2.20 action=accpet
   [admin@MikroTik] > ip firewall filter add chain=forward src-address=192.168.2.0/24 action=reject reject-with=icmp-host-unreachable
3. Memblok client melalui Mac Address
   Untuk melihat user yang sedang aktif
   [admin@MikroTik] > ip arp print

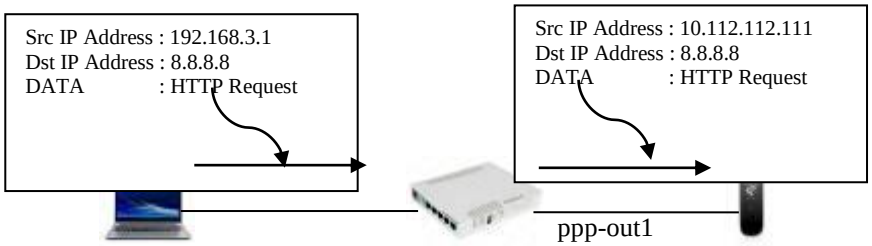
```
[admin@MikroTik] > ip arp print
Flags: X - disabled, I - invalid, H - DHCP, D - dynamic, P - published
 #   ADDRESS         MAC-ADDRESS       INTERFACE
 0 D 192.168.2.10    60:EB:69:72:A7:83 ether2
[admin@MikroTik] >
```

Gambar 3.3 Tampilan Client aktif

   Perintah memblock client melalui Mac Address
   [admin@MikroTik] > ip firewall filter add chain=forward action=drop src-mac-address=60:EB:69:72:A7:83
   Maka ketika user ingin mengakses internet tidak akan berhasil karena telah diblokir oleh administrator.

B. NAT (*Network Address Translation*)

Fungsi firewall yang bertugas melakukan perubahan IP Adress dari komputer user seolah-oleh berasal dari router. Tujuannya agar server di internet hanya mengetahui bahwa yang mengakses internet adalah router.



Gambar 3.4 Masquerade ke ppp-out1

[admin@MikroTik] > ip firewall nat add chain=srcnat out-interface=ppp-out1 action=masquerade

Perintah diatas memerintahkan "jika komputer user akan mengakses internet, beradalah pada ppp-out1, chain=srcnat berfungsi gantilah IP Address pengirim 192.168.3.1 menjadi IP Address di ppp-out1 jika ingin menuju internet.

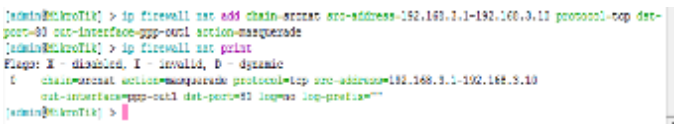
Berikut adalah perintah masquerade untuk menentukan komputer user yang dapat mengakses internet.

[admin@MikroTik] > ip firewall nat add chain=srcnat src-address=192.168.3.1-192.168.3.20 out-interface=ppp-out1 action=masquerade

untuk menghapus perintah nat sebelumnya

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

1. Perintah masquerade agar user hanya mendapatkan layanan browsing (HTTP) berikut adalah perintah nya
   [admin@MikroTik] > ip firewall nat add chain=srcnat src-address=192.168.3.1-192.168.3.10 protocol=tcp dst-port=80 out-interface=ppp-out1 action=masquerade



Gambar 3.5 Konfigurasi Masquerade ke ppp-out1

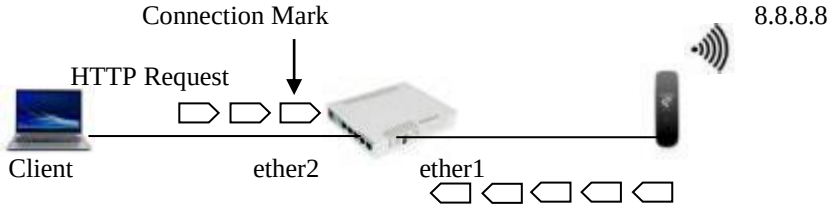
2. Jika ingin komputer user dapat melakukan ping (Protokol ICMP) ke situs internet
   [admin@MikroTik] > ip firewall nat add chain=srcnat src-address=192.168.3.7 protocol=icmp out-interface=ppp-out1 action=masquerade

3. Perintah Masquerade dengan fungsi waktu, yaitu membatasi akses terhadap suatu layanan misalnya layanan HTTP/HTTPS , berikut adalah perintahnya

[admin@MikroTik] > ip firewall nat add chain=srcnat src-address=192.168.3.1-192.168.3.50 protocol=tcp dst-port=80,443 time=08:00:00-23:00:00,sun out-interface=ppp-out1 action=masquerade

C. Mangle

Mangle merupakan salah satu fitur pada firewall Router Mikrotik yang digunakan untuk memberi tanda (*mark*) pada paket data.



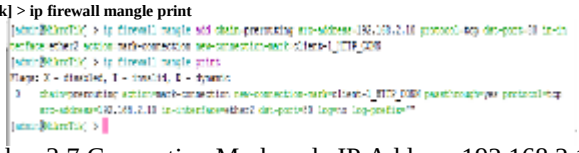
Gambar 3.6 Connection Mark pada HTTP Request

1. Connection Mark

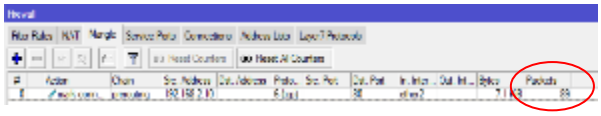
Jenis marking yang digunakan untuk menandai adanya suatu koneksi, perintahnya adalah sebagai berikut

[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=192.168.2.10 protocol=tcp dst-port=80 in-interface=ether2 action =mark-connection=client-1_HTTP_CONN

[admin@MikroTik] > ip firewall mangle print



Gambar 3.7 Connection Mark pada IP Address 192.168.2.10



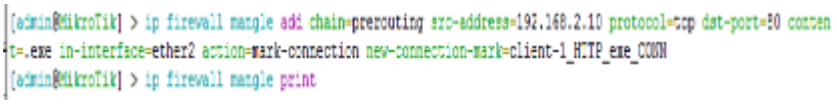
Gambar 3.8 Hasil Connection Mark pada IP Address 192.168.2.10

Jika ingin melakukan marking pada semua jenis koneksi dari client tanpa melihat jenis koneksi yang dilakukannya, maka tidak perlu memasukkkan parameter protocol dan dst-port

[admin@MikroTik] > #ip firewall mangle add chain=prerouting src-address=192.168.2.10 in-interfaces=ether2 action=mark-connection new-connection-mark=client-1_CONN

Jika ingin melakukan marking terhadap aktifitas download untuk file extensi .exe, perintah yang dapat digunakan adalah sebagai berikut.

[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=192.168.2.10 protocol=tcp dst-port=80 content=.exe in-interface=ether2 action=mark-connection new-connection-mark=client-1_HTTP_exe_CONN

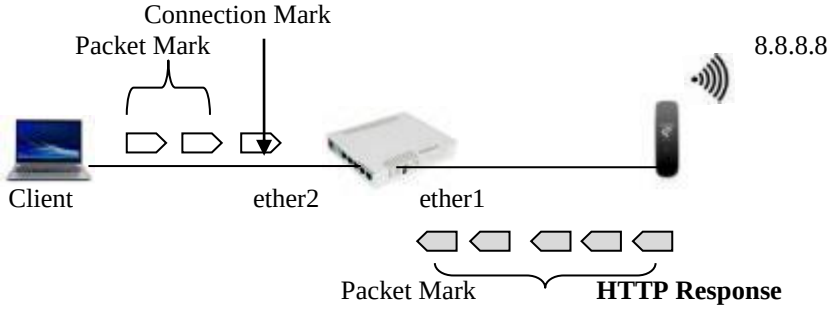


Gambar 3.9 Konfigurasi Connection Mark content

2. Packet Mark

Melakukan marking pada paket-paket lanjutan setelah paket pertama tadi yaitu Connection Mark

HTTP Request



Gambar 3.10 Keseluruhan stream data HTTP dari komputer client

Dari gambar diatas memperlihatkan komputer client yang sedang melakukan aktifitas download dari suatu Web Server di Internet. Pada gambar diatas jumlah paket response lebih banyak (5 packet) dari jumlah paket request (3paket). Karena pada umumnya *traffic* download lebih besar dari *traffic* upload.

Terlihat bahwa *Connection Mark* digunakan untuk melakukan *marking* pada paket pertama. Sedangkan *Packet Mark* digunakan untuk melakukan *marking* pada paket-paket selanjutnya.

Berikut adalah cara membuat marking pada keseluruhan *traffic* (baik upload aupun download) dari seluruh client yang ada di jaringan 192.168.2.0/24

1. Membuat Connection Mark

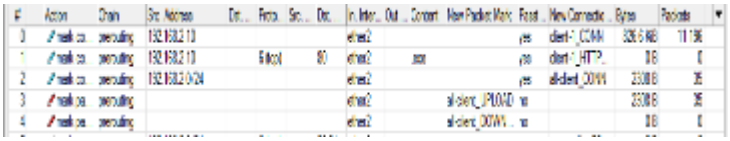
```
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=192.168.2.0/24 in interface=ether2 action-mark-connection new-
                   connection-mark=all-client_CONN passthrought=no
```

2. Selanjutnya membuat marking terhadap keseluruhan *traffic* upload

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting connection-mark=all-client_CONN in-interface=ether2 action=mark-packet new-
                   packet-mark=all-client-UPLOAD passthrough=no
```

3. Selanjutnya membuat marking terhadap keseluruhan *traffic* download

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting connection-mark=all-client_CONN in-interface=ppp-out1 action=mark-packet
                   new-packet-mark=all-client-DOWNLOAD passthrough=no
```



Gambar 3.11 Hasil konfigurasi Connection Mark

Berikut adalah cara membuat marking yang dipisahkan menjadi dua bagian besar, marking pertama ditujukan untuk akses internet biasa dari keseluruhan komputer client. Akses Internet ini sudah termasuk layanan HTTP/HTTPS, FTP, DNS dan lain-lain. Sedangkan marking kedua ditujukan untuk aktifitas download file-file tertentu, misalnya file dengan ekstensi .exe, .mp3, .mp4, .rar, .flv, dan lain-lain.

1. Tahap pertama adalah membuat Connection Mark

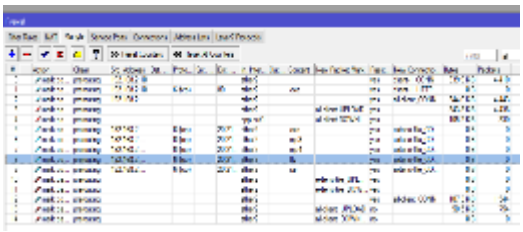
```
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=192.168.2.0/24 protocol=tcp dst-port=20,21,80 in-interface=ether2
                   content=.exe action=mark-connection new-connection-mark=extensi-file_CONN passthrough=yes
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=192.168.2.0/24 protocol=tcp dst-port=20,21,80 in-interface=ether2
                   content=.mp3 action=mark-connection new-connection-mark=extensi-file_CONN passthrough=yes
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=192.168.2.0/24 protocol=tcp dst-port=20,21,80 in-interface=ether2
                   content=.mp4 action=mark-connection new-connection-mark=extensi-file_CONN passthrough=yes
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=192.168.2.0/24 protocol=tcp dst-port=20,21,80 in-interface=ether2
                   content=.flv action=mark-connection new-connection-mark=extensi-file_CONN passthrough=yes
[admin@MikroTik] > ip firewall mangle add chain=prerouting src-address=192.168.2.0/24 protocol=tcp dst-port=20,21,80 in-interface=ether2
                   content=.rar action=mark-connection new-connection-mark=extensi-file_CONN passthrough=yes
```

2. Selanjutnya membuat Packet Mark berdasarkan Connection Mark tadi

```
[admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=extensi-file_CONN action=mark-packet
                   new-packet-mark=extensi-file_UPLOAD
[admin@MikroTik] >  ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=extensi-file_CONN action=mark-packet
                   new-packet-mark=extensi-file_DOWNLOAD
```

3. Selanjutnya membuat marking untuk *traffic* upload dan download

```
[admin@MikroTik] > #ip firewall mangle add chain=prerouting in-interface=ether2 action=mark-connection new-connection-mark=all-
                   client_CONN passthrough=yes
[admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=all-client_CONN action=mark-packet new-
                   packet-mark=all-client-UPLOAD passthrough=no
[admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=all-client_CONN action=mark-packet new-
                   packet-mark=all-client-DOWNLOAD passthrough=no
```

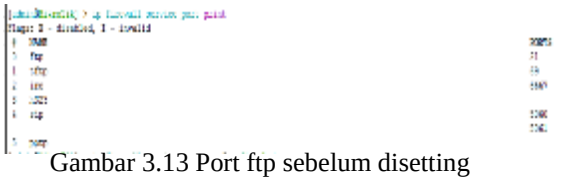


Gambar 3.12 Hasil Konfigurasi Packet Mark ether2

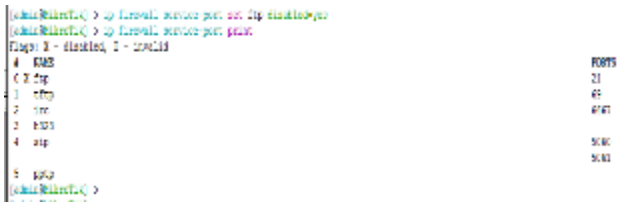
D. Service Port

Berikut adalah perintah jika ingin tidak mengaktifkan salah satu port atau mengubah nama port yang ada

```
[admin@MikroTik] > ip firewall service-port print
[admin@MikroTik] > ip firewall service-port set ftp disabled=yes
[admin@MikroTik] > ip firewall service-port print
```



Gambar 3.13 Port ftp sebelum disetting



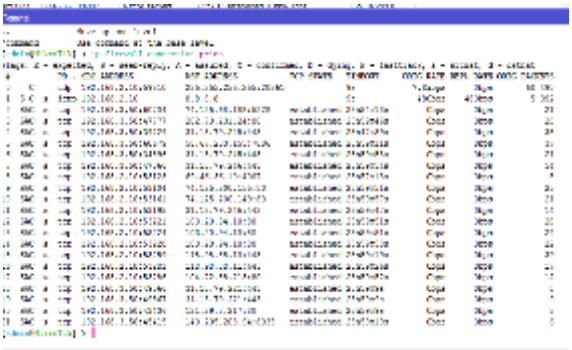
Gambar 3.14 Port ftp setelah disetting

E. Connections

1. Connection Tracking adalah "jantung" dari firewall, mengumpulkan informasi tentang active connections.
2. Dengan mendisable connection tracking router akan kehilangan fungsi NAT, filter rule dan mangle.
3. Setiap connection tracking membaca pertukaran traffic 2 arah (src dan dst address).
4. Connection tracking membutuhkan CPU resources (disable saja jika kita tidak menggunakan firewall).

Berikut adalah perintah untuk mengetahui koneksi yang terjadi

[admin@MikroTik] > ip firewall connection print

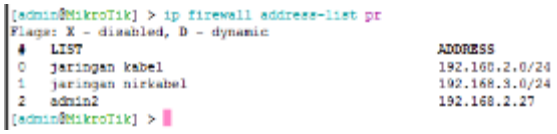


Gambar 3.15 IP Firewall Connection

5. Address List

Fitur ini dapat digunakan untuk keperluan deklarasi IP Address maupun untuk kepentingan *logging* (pencatatan aktifitas jaringan). Berikut adalah penggunaan Address List untuk pendeklarasian IP Address dalam jaringan.

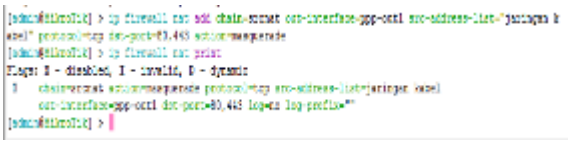
[admin@MikroTik] > ip firewall address-list add address=192.168.2.0/24 list="jaringan kabel"
[admin@MikroTik] > ip firewall address-list add address=192.168.3.0/24 list="jaringan nirkabel"
[admin@MikroTik] > ip firewall address-list add address=192.168.2.27 list="admin2"



Gambar 3.16 Hasil Konfigurasi Address List

Jika ingin melakukan konfigurasi pada bagian firewall, tidak perlu lagi menuliskan IP Address. Berikut adalah penggunaan Address List pada konfigurasi NAT.

[admin@MikroTik] > #ip firewall nat add chain=srcnat out-interface=ppp-out1 src-address-list="jaringan kabel" protocol=tcp dst-port=80,443 action=masquerade



Gambar 3.17 Penggunaan Address List pada konfigurasi NAT

6. Layer 7 Protocol

   Cara memblokir situs dengan memanfaatkan kombinasi Layer 7 Protocol dan Firewall Filter

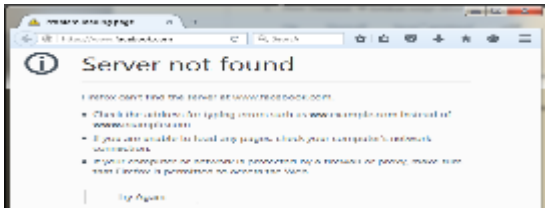
1. New Terminal → ketikan script dibawah ini

   [admin@MikroTik] > ip firewall layer7-protocol add name=facebook regexp="^.+(facebook.com).*\$"

2. Selanjutnya

   [admin@MikroTik] > ip firewall filter add chain=forward layer7-protocol=facebook action=drop

3. Maka ketika komputer client hendak mengakses situs tersebut tidak akan bisa terbuka.



Gambar 3.18 Blokir situs website

4. KESIMPULAN

Adapun kesimpulan yang diperoleh penulis adalah sebagai berikut :

a. Penggunaan Router Mikrotik pada jaringan terbukti mampu meningkatkan sistem firewall jaringan.
b. Penggunaan fitur firewall pada jaringan memungkinkan administrator jaringan dalam memonitoring akses internet dari setiap user.
c. Penggunaan firewall pada jaringan dapat mencatat setiap kejadian yang terjadi pada jaringan sehingga dapat melakukan pendeteksian dini terhadap serangan yang ada.
d. Dengan adanya fungsi NAT (*Network Address Translation*) dapat mengamankan IP Address Private client sehingga yang terlihat oleh server yang ada di internet yaitu IP Address Public.

UCAPAN TERIMA KASIH

Terima Kasih di tujukan kepada Para Dosen Pembimbing , Penguji sdr. Epi Rahmat Putra Gulo yang telah membinmbing dengan baik dalam penyelesaian tulisan ini.

REFERENSI

[1] Imam Riadi, 2011, "*Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik*". Jurnal Sistem Informasi Universitas Ahmad Dahlan, Yogyakarta.
[2] Imam Riadi, 2011, "*Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik*". Jurnal Sistem Informasi Universitas Ahmad Dahlan, Yogyakarta.
[3] Towidjojo, Rendra. 2016. Mikrotik Kung Fu : Kitab 3. Jakarta: JASAKOM
[4] Towidjojo, Rendra. 2016. Mikrotik Kung Fu : Kitab 4. Jakarta: JASAKOM
[5] Azis, Catur. 2008. Panduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik Routers. Yogyakarta: Andi.
[6] Listianto, V. 2011. Teknik Jaringan Komputer, Jakarta: Prestasi Pustaka Publisher.