# 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	ABSTRACT
Article history: Received Jun 06 <sup>th</sup> , 2021 Revised Jul 23 <sup>th</sup> , 2021 Accepted Jul 30 <sup>th</sup> , 2021	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
<b>Keyword:</b> Firewall Packet Filtering Router Microtik	pertukaran paket data yang terjadi harus melewati firewall.
	Copyright © 2021 STMIK Triguna Dharma. All rights reserved.

### **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



## 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 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
- Memblok client melalui Mac Address Untuk melihat user yang sedang aktif

[admin@MikroTik] > ip arp print

[admin8MikroTik] > ip arp print Flags: X - disabled, I - invalid, H - DHCP, D - dynamic, P - published # ADDRESS NAC-ADDRESS INTERFACE 0 D 192.168.2.10 60:EB:69:72:A7:83 ether2 [admin8MikroTik] > 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 pppout1, 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

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

ito Rale	BAT N	ngla Servi	e Petal ()	o siccia o	Niden Ltb	Laye 7 Petercele			
• -	8 2	r: 7	D3 Nood	Counters	ao Heset Al C	burters			$\sim$
2 /	citer	Chain	Se.N	den Dr./	dores Pete	Se Pet Da	/.Pat in Inter 1	Dal H., Becc. /	Pation

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=prevouting src-address=192.168.2.10 in-interfaces=ether2 action=mark-connection newconnection-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 ininterface=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** 



<sup>[</sup>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

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 newconnection-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 newpacket-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

Ę.	Action	Chain	Ste Address	Dt	Ritta.	Sc.,	Dr.	h, Ister, Du	t., Contert	New Packet Mark	hast.	New Correction	Bytes	Pacints	۳
1	/ tek p.	peruling	192,168,2,10					ete2			(55	dert-1,000M	8266 MB	111%	
1	/ neik co.	pendig	192,168,210		5 tol		80	eter2	10		60	dent ( HTP.	18	[	
2	/ telt (a.	peruling	1921682024					eter?			(85	alder(00%)	2308 B	ž	
3	/ nak pa	peouting						eter2		aliders_UPLOAD	10		2308 B	ž	
4	/ nek pa.	perculing						ehei?		alkiet 00WV	10		18	1	
										-					

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=..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 [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-mark=extensi-file\_CONN passthrough=yes 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
- 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=allclient\_CONN passthrough=yes [admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=all-client\_CONN action=mark-packet new-

[admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=all-client\_CONN action=mark-packet newpacket-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-

admin@MikroTik] > ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=all-client\_CONN action=mark-packet newpacket-mark=all-client-DOWNLOAD passthrough=no

•												
		C T	So Long Control	46.944	Conten							
	50	0.0	St Aber 34	Por 18	- Kr	6. INC. 34	Court	He factor to	feet.	New Connector	Rei I	hde i
5	week to.	10000	22.042.0			100			101	205 00 8	10(6)	
1	stank to	(money)	12,082,0	68/54	× 1	100	0.0		124	tion 1000	85	
:	stank to	printing.	12,040			aler all			124	string (MR	ALC: NO	- 14
۰.	d'ank to	10000				start .		al free UP 140	27.8		ALC: NO.	
1	d'arders.	10000				79.96		al first \$272.4	24		10.161	
۲.	Andres	10000	101401	E berg	717	der!	101		24	minut ling 70	84	
	Zarke.	1000	1010	E le s	212	day 1	- <b>1</b>		24	minut ling 11	84	
έ.	Zank et al.	in the second second	10107	E laur	202	decision in the	- mid -		Sec. 1	ada at the 324	8.	
	Cash one	PT-SAV	10102	I have been	2/7	dist.	- N		798	ada a dia 528.	21	
	Cash one	STARS.	1427424	Billion 1	275	din a			191	where the U.A.		
	Casher	in the second second				des -		elective JPL.	÷	-		
i .	Cash in	STATES.				dina -		where the Although	-			
	Cost 21	10000				de's			-	abdex 00%	107180	- 54
5	Pack 14	120000				phane in the		Molect PDAD	10		9:65	29
	d'and to	10000				start .		Mining Yillia	-			

Gambar 3.12 Hasil Konfigurasi Packet Mark ether2

#### D. Service Port

2

3.

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

_det_lift(reflit) > op forvall verder part parts finger 2 - drambed 1 - doulld + 7000 5 fep 1 trip 2 trip 2 trip	20275 21 23 2547
b lake	5060 5061
Gambar 3.13 Port ftp sebelum disetting	
<pre>[ckmi@timfle( &gt; up firmed) menter per set fit finitis/yer [ckmi@timfle( &gt; up firmed) menter per prim Figur 3 - dissiled, 1 - iraclid 4 FMS C 2 fep 1 - thm 2 - tm</pre>	F0675 21 65 6167
2 E03 4 atp	5080
s spige (since Related L.C. 5	2.61

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

10	-									
				free op oor feerland						
100	CA4C	2		are company at the par-	e James					
100	le i eiji	÷.,	-7124	<ul> <li>(a) (p) (thread) it concerns.</li> </ul>	ter peters					
114	gan a	٤-	10,000 (M	сес, и – неер-серчу, А	- assured, 5 - contains	ac, o - aja	ag. 21 - 2003	Clack, A -	abcast, d - a	ALC: NO
			20.0	Chill AMERICAN	BOP 2007BOS	TCP SIMIS	1140007	CODC BATE	2018, DATE 000	C DARKING
2	. C		sale.	142.040.0.00.00.00000	216.36.251.361.2516		3.	3. Except	May 10	NO 180
	5.0	3	1000	102.160.2.10	8.5.0.6		57	4500aa	403656	5 352
1	ALC: NO		-	142.183.0.00480194	10.118.00.009.0078	re tablication	23 @1+03a	Cape	Sigma .	21
- 2	340		110	192.160.3.50:47777	202.10.201.24100	arrabit free	100030468	Cas	1000	20
	84C		1.0	152.188.3.80.00024	21.12.15.218.143	relabilitated	22 M C 12 M	C 199	Sec. 1	2.4
	- 14		125	242.146.3.30360.03	20.41.210.1207.000	PLUE STREET SHO	2.2.9511	Coga	1004	21
	240		100	110.100.0.000000000	211-02-12-2004042	recard to set	20.00 100.00	- C	and the second sec	21
1	-			142.140.1.00147.000	21.21.76.2161141	PROPERTY OF COMPANY	2.2.47.18	- Coga	2604	24
	20		100	110.100.0.10000100	85.4C.0C.154381	result in the	22202200120	Color.	Contract of the local division of the local	
	896.			142.141.2.10103104	34,125,286,1255,59	AN INDULATION	212040018	C	26.04	2.
	940		200	102.0012.0015100	14.115.100.145:00	trabitine.	210100179	Cer	Office of	21
	ANK.		-	142.141.2.10.00180	21.11.99.218.193	re Lab. La ter.	21021010	C.que	100	
	344.		111	192.100.2.10151821	202.42.24.10.26	STINCLINES.	119034112	Cons	1000	20
	ALC: NO		-	192.102.2.10102124	100.70.94.10.40	re tal 1 is net	27.01.01	C	100	21
	100		111	192.146.0.00151226	212.12.12.14.10.20	PLANE COLLEGE	2.2.17.10	Cost	1000	
	100			192.100.2.10102.00	10.00.00.00000	A Later and	22.00	C		31
	100			100.000.0.0000000		arraditarsed	2.2.95210	Copa -	and a second	
-	100	1		112.100.2.1010.00	101.12.01.20.000	result in the	20.00 100 20	- m	100	
1	100	1	-+	121 141 1 10 10 10	11.11.11.11.11.11.11.1	AND DECK OFFICE	2.2.1		and a second	
12	-		10	The state of second second	11-15-15-C-1945		1000		100	
11	110		-	100 0.00 0.00 00 00 000	AND THE REPORT OF	and the second second	ALC: NOT THE REAL PROPERTY OF		100	
1	-		111	1201000131003404040	243.435.853.5655335	1111001111000	2000000100	Const	100	

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"

[ad Fla	<pre>nin@MikroTik] &gt; ip firewall address-list pr gs: X = disabled, D = dynamic</pre>	
•	L157	ADDRESS
0	jaringan kabel	192.160.2.0/24
1	jaringan nirkabel	192.168.3.0/24
2	admin2	192.168.2.27
Lad	nin8NikroTikl >	



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

```
[sdm:diirolk] > tp firmeall not odd chain-sommat cot-interface-ppp-ontl suc-address-list-"paingen k
walf protocol-map for-point 0.45% addicermemperade
[sdm:diirolk] > tp firmeall not print
Exampl 4 - disabled, I - invalid, D - fyrmain
1 - disabled, I - invalid, D - fyrmain
2 - disabled, I - invalid, D - fyrmain
3 - disabled, I - invalid, D - fyrmain
4 - disabled, I - invalid, D - fyrmain
5 - disabled, I - invalid, D - fyrmain
5 - disabled, I - invalid, D - fyrmain
6 - invariant-sopp-cont dot perm-b0,45% log-ma log-profix="""
```

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  $\rightarrow$  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.