

# Pengenalan FIREWALL



Organized By : Politeknik Astra

# Outline Materi

**Pada materi ini akan dibahas mengenai :**

- ❖ Firewall Overview
- ❖ Port Services & Protocol
- ❖ Firewall Chain
- ❖ Action Filter
- ❖ Implementasi Firewall Basic





# Firewall MikroTik

- ❖ Pada RouterOS MikroTik terdapat sebuah fitur yang disebut dengan 'Firewall'.
- ❖ Fitur ini biasanya banyak digunakan untuk melakukan :
  - ✓ Filtering akses (Filter Rule),
  - ✓ Forwarding (NAT),
  - ✓ Menandai koneksi maupun paket dari trafik data yang melewati router (Mangle).
- ❖ Terdapat sebuah parameter utama pada rule di fitur firewall ini yaitu 'Chain'.
- ❖ Parameter ini memiliki kegunaan untuk menentukan jenis trafik yang akan di-manage pada fitur firewall dan setiap fungsi pada firewall seperti **Filter Rule**, **NAT (Network Address Translation)**, **Mangle** memiliki opsi chain yang berbeda.

# Port Services & Protocol

Beberapa port yang sering digunakan dalam jaringan :

Port	Service
80/tcp	HTTP
443/tcp	HTTPS
22/tcp	SSH
23/tcp	Telnet
20,21/tcp	FTP
8291/tcp	WinBox
5678/udp	MikroTik Neighbor Discovery
20561/udp	MAC WinBox

# Firewall Filter Chain – Aliran Data

Tiga aturan dasar packet flow :

- Input – **KE** router                      contoh : ping ke router
- Output – **DARI** router                      contoh : ping router ke internet
- Forward – **MELEWATI** router                      contoh : user mengakses internet



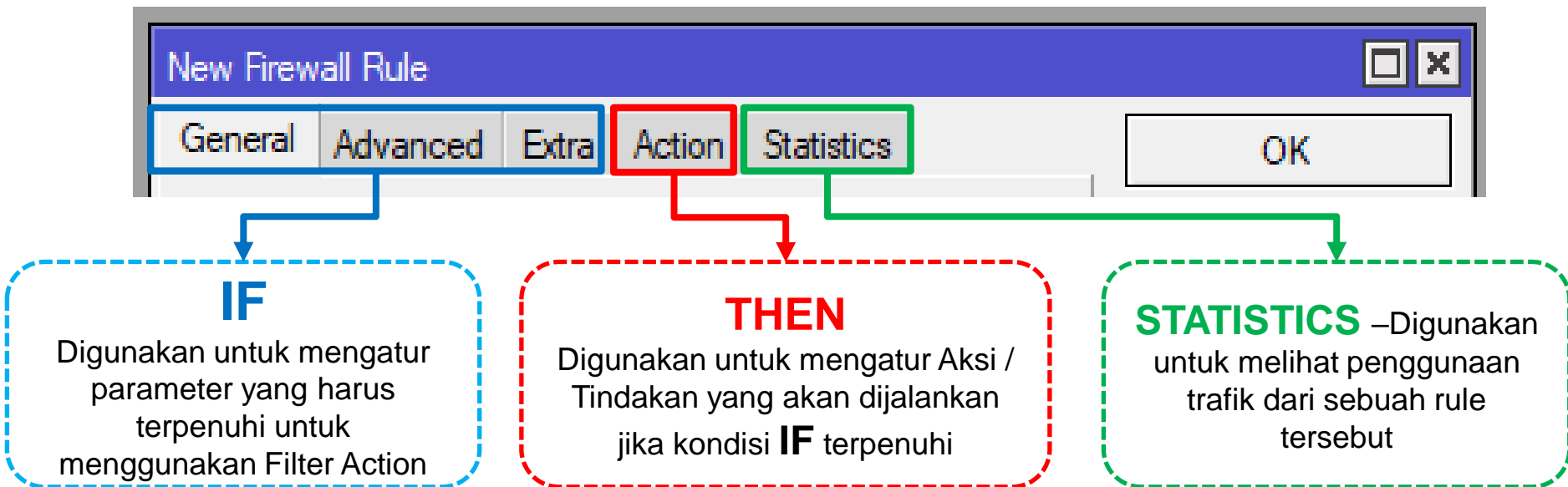
# Penggunaan Firewall Filter

❖ Prinsip **IF** ..... **Then** .....

- **IF** (Jika) paket memenuhi syarat kriteria yang kita buat.
- **Then** (maka) action apa yang akan kita berikan ke paket tersebut.

❖ Di firewall Filter Rule **IF condition** ada dimenu (**General**, **Advanced** dan **Extra**)

❖ sedangkan **Then condition** ada dimenu **action**



# Penggunaan Firewall Filter - IF

Firewall

Filter Rules NAT Mangle Raw Service Ports Connection

+ - ✓ ✗ [Icon] [Icon] 00 Reset Counters 00

# Action Chain

New Firewall Rule

General Advanced Extra Action Statistics

Chain: forward

Src. Address: [Field]

Dst. Address: [Field]

Protocol: [Field]

Src. Port: [Field]

Dst. Port: [Field]

Any. Port: [Field]

P2P: [Field]

In. Interface: [Field]

Out. Interface: [Field]

**Src. Address** Merupakan IP Address sumber (jaringan private / LAN)

**Dst. Address** Merupakan IP Address tujuan (jaringan internet)

**Protocol** Merupakan protocol yang digunakan seperti contoh TCP / UDP / ICMP

**Src Port** Merupakan port sumber yang digunakan

**Dst Port** Merupakan port tujuan yang digunakan

**In Interface** Interface yang digunakan untuk trafik datang dari internet ke LAN

**Out Interface** Interface yang digunakan untuk trafik keluar dari LAN ke internet

# Penggunaan Firewall Filter - THEN

**ACCEPT** : Paket diterima dan tidak melanjutkan membaca baris berikutnya.

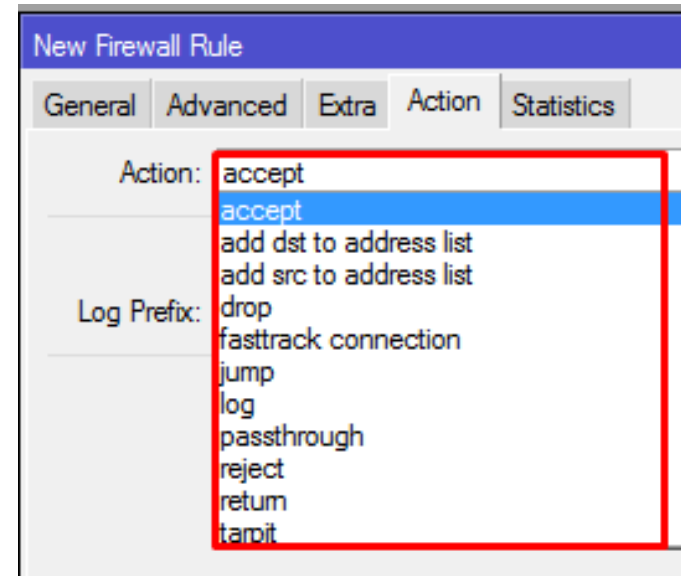
**DROP** : Menolak paket secara diam-diam (tidak mengirimkan pesan penolakan ICMP).

**REJECT** : Menolak paket dan mengirimkan pesan penolakan ICMP.

**JUMP** : Melompat ke chain lain yang ditentukan oleh nilai parameter jump-target.

**TARPIT** : Menolak, tetapi tetap menjaga TCP connection yang masuk (membalas dengan SYN/ACK untuk paket TCP SYN yang masuk).

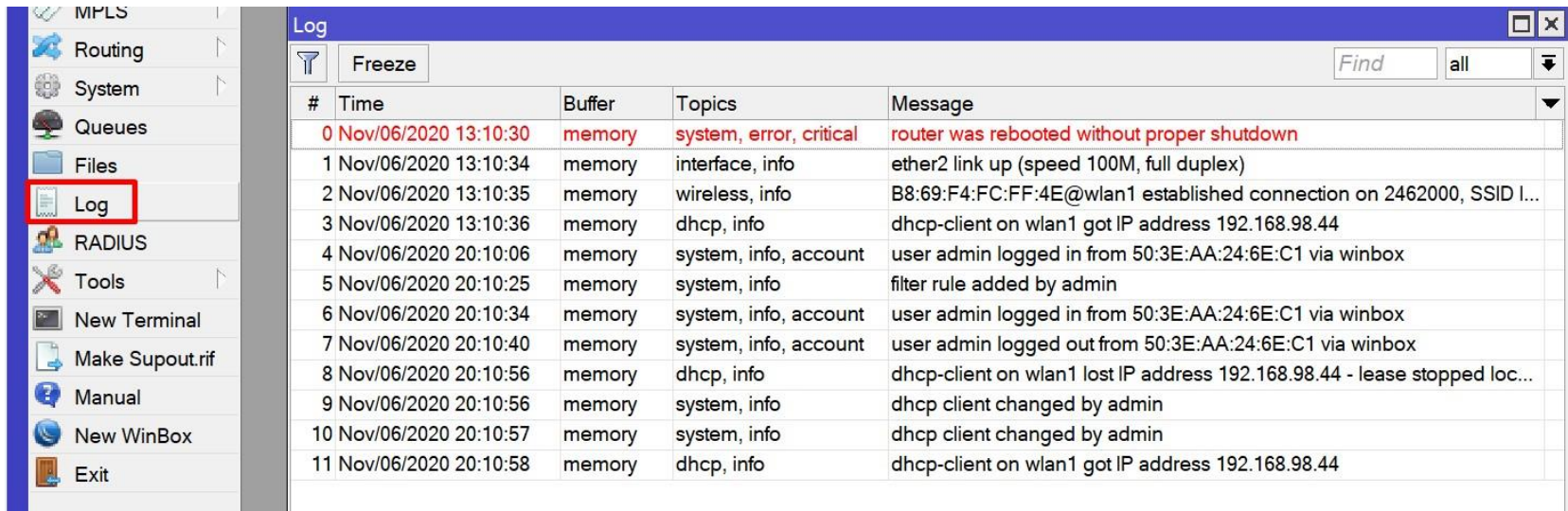
**LOG** : Menambahkan informasi paket data ke log.





# Firewall LOG

- ❖ Log merupakan fitur yang digunakan untuk menampilkan beberapa informasi / aktivitas yang ada pada router.



#	Time	Buffer	Topics	Message
0	Nov/06/2020 13:10:30	memory	system, error, critical	router was rebooted without proper shutdown
1	Nov/06/2020 13:10:34	memory	interface, info	ether2 link up (speed 100M, full duplex)
2	Nov/06/2020 13:10:35	memory	wireless, info	B8:69:F4:FC:FF:4E@wlan1 established connection on 2462000, SSID I...
3	Nov/06/2020 13:10:36	memory	dhcp, info	dhcp-client on wlan1 got IP address 192.168.98.44
4	Nov/06/2020 20:10:06	memory	system, info, account	user admin logged in from 50:3E:AA:24:6E:C1 via winbox
5	Nov/06/2020 20:10:25	memory	system, info	filter rule added by admin
6	Nov/06/2020 20:10:34	memory	system, info, account	user admin logged in from 50:3E:AA:24:6E:C1 via winbox
7	Nov/06/2020 20:10:40	memory	system, info, account	user admin logged out from 50:3E:AA:24:6E:C1 via winbox
8	Nov/06/2020 20:10:56	memory	dhcp, info	dhcp-client on wlan1 lost IP address 192.168.98.44 - lease stopped loc...
9	Nov/06/2020 20:10:56	memory	system, info	dhcp client changed by admin
10	Nov/06/2020 20:10:57	memory	system, info	dhcp client changed by admin
11	Nov/06/2020 20:10:58	memory	dhcp, info	dhcp-client on wlan1 got IP address 192.168.98.44

- ❖ Kita dapat membuat atau menambahkan catatan aktivitas apa saja sesuai yang diinginkan melalui firewall filter dengan menggunakan action **log**.



# NAT

- ❖ NAT (**Network Address Translation**) merupakan metode yang digunakan untuk menghubungkan banyak komputer ke jaringan Internet dengan menggunakan satu / lebih alamat IP.
- ❖ NAT digunakan untuk ketersediaan alamat IP Public
- ❖ Prinsip NAT sama seperti Filter Rule, bekerja dengan “IF-THEN”.



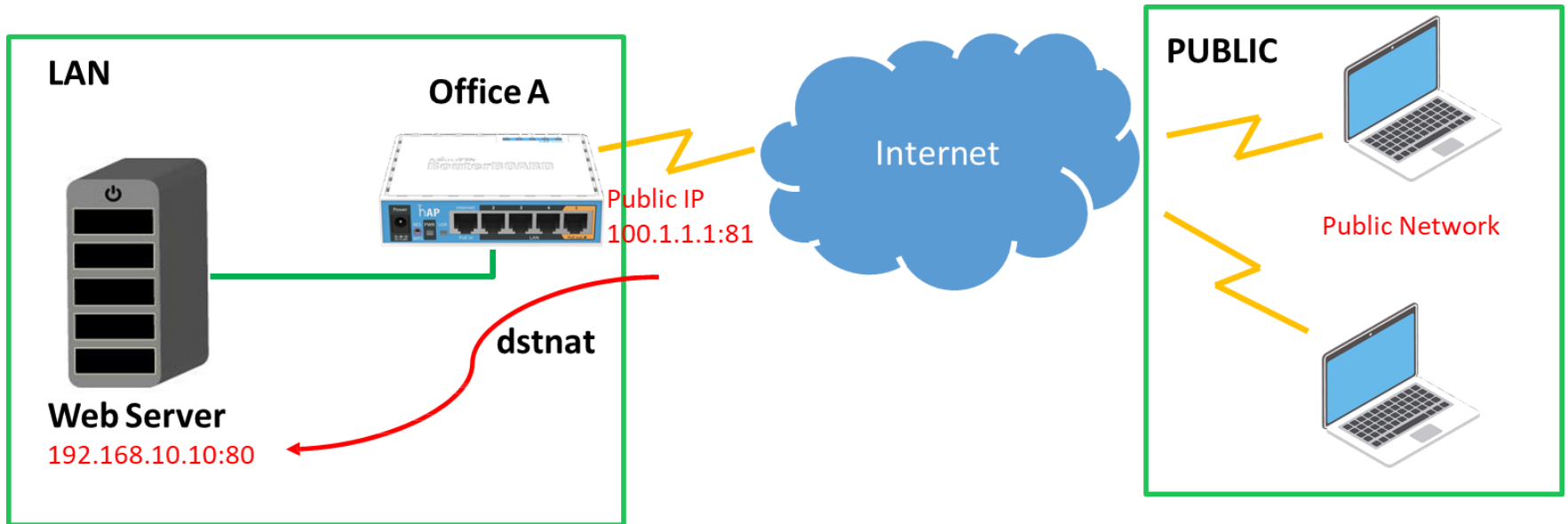
# NAT

Di Mikrotik terdapat 2 type NAT :

- **Srcnat**, digunakan ketika client yang ada di dalam router ingin keluar (Internet).
  - **Masquerade** : digunakan untuk menghubungkan jaringan lokal ke internet menggunakan IP public dynamic.
  - **Src-nat** : digunakan untuk menghubungkan jaringan lokal ke internet menggunakan IP public static.
- **Dstnat**, digunakan ketika client di internet ingin mengakses jaringan local dari internet
  - **Dst-nat** : digunakan ketika akan mengakses jaringan lokal melalui internet (port forwarding). → melempar traffik ke luar router.
  - **Redirect** : digunakan ketika akan membelokan traffic ke router itu sendiri. contoh : hotspot, webproxy, dns server router dll

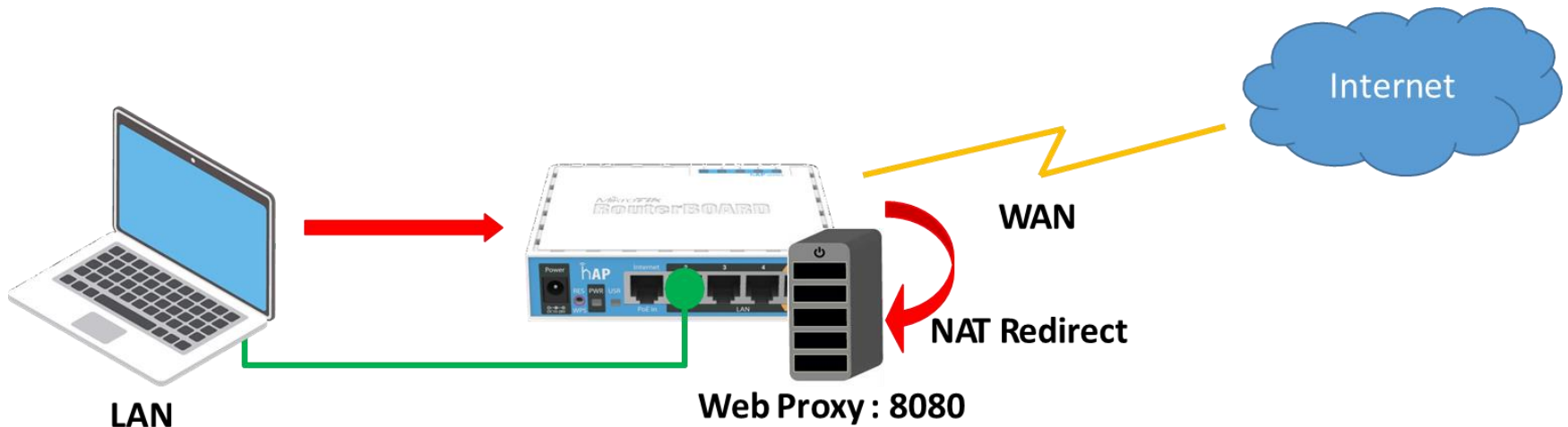
# Firewall DST-NAT

- ❖ DSTNAT digunakan untuk mengakses host/service yang ada di Lokal melalui Public Internet.



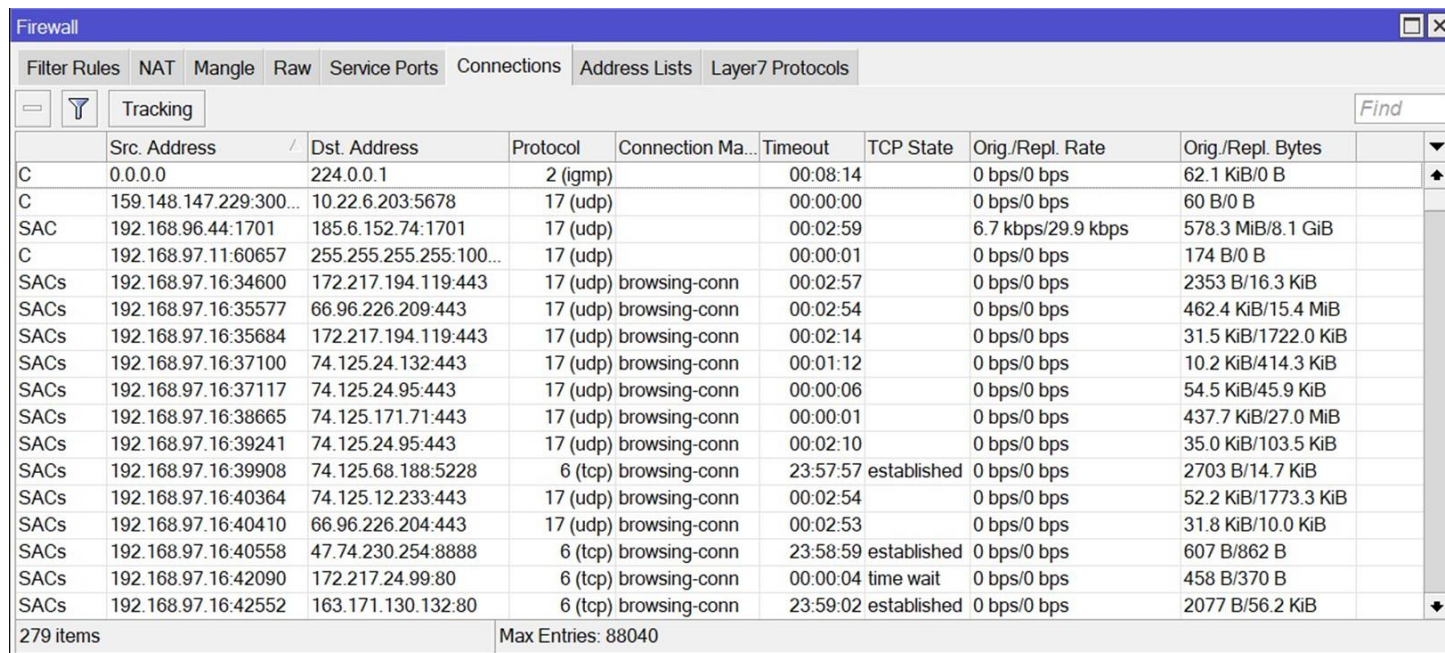
# Firewall Redirect

- ❖ Merupakan action yang digunakan untuk mengarahkan suatu paket kedalam spesifik servis / port yang ada pada router. (DNS, Web Proxy).
- ❖ Redirect hanya bisa digunakan apabila kita menggunakan chain dstnat



# Firewall Connection Tracking

- ❖ Connection Tracking berisi informasi koneksi (source, destination IP, port, protocol yang sedang digunakan)
- ❖ Harus diaktifkan bila kita akan menggunakan beberapa service Firewall.
- ❖ IP > Firewall > Connections > Tracking



	Src. Address	/	Dst. Address	Protocol	Connection Ma...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes	
C	0.0.0.0		224.0.0.1	2 (igmp)		00:08:14		0 bps/0 bps	62.1 KiB/0 B	
C	159.148.147.229:300...		10.22.6.203:5678	17 (udp)		00:00:00		0 bps/0 bps	60 B/0 B	
SAC	192.168.96.44:1701		185.6.152.74:1701	17 (udp)		00:02:59		6.7 kbps/29.9 kbps	578.3 MiB/8.1 GiB	
C	192.168.97.11:60657		255.255.255.255:100...	17 (udp)		00:00:01		0 bps/0 bps	174 B/0 B	
SACs	192.168.97.16:34600		172.217.194.119:443	17 (udp) browsing-con		00:02:57		0 bps/0 bps	2353 B/16.3 KiB	
SACs	192.168.97.16:35577		66.96.226.209:443	17 (udp) browsing-con		00:02:54		0 bps/0 bps	462.4 KiB/15.4 MiB	
SACs	192.168.97.16:35684		172.217.194.119:443	17 (udp) browsing-con		00:02:14		0 bps/0 bps	31.5 KiB/1722.0 KiB	
SACs	192.168.97.16:37100		74.125.24.132:443	17 (udp) browsing-con		00:01:12		0 bps/0 bps	10.2 KiB/414.3 KiB	
SACs	192.168.97.16:37117		74.125.24.95:443	17 (udp) browsing-con		00:00:06		0 bps/0 bps	54.5 KiB/45.9 KiB	
SACs	192.168.97.16:38665		74.125.171.71:443	17 (udp) browsing-con		00:00:01		0 bps/0 bps	437.7 KiB/27.0 MiB	
SACs	192.168.97.16:39241		74.125.24.95:443	17 (udp) browsing-con		00:02:10		0 bps/0 bps	35.0 KiB/103.5 KiB	
SACs	192.168.97.16:39908		74.125.68.188:5228	6 (tcp) browsing-con		23:57:57	established	0 bps/0 bps	2703 B/14.7 KiB	
SACs	192.168.97.16:40364		74.125.12.233:443	17 (udp) browsing-con		00:02:54		0 bps/0 bps	52.2 KiB/1773.3 KiB	
SACs	192.168.97.16:40410		66.96.226.204:443	17 (udp) browsing-con		00:02:53		0 bps/0 bps	31.8 KiB/10.0 KiB	
SACs	192.168.97.16:40558		47.74.230.254:8888	6 (tcp) browsing-con		23:58:59	established	0 bps/0 bps	607 B/862 B	
SACs	192.168.97.16:42090		172.217.24.99:80	6 (tcp) browsing-con		00:00:04	time wait	0 bps/0 bps	458 B/370 B	
SACs	192.168.97.16:42552		163.171.130.132:80	6 (tcp) browsing-con		23:59:02	established	0 bps/0 bps	2077 B/56.2 KiB	

279 items Max Entries: 88040



# Firewall Connection Tracking

Bila **connection tracking mati**, beberapa fitur firewall tidak akan berfungsi sebagai berikut :

❖ NAT

❖ Firewall :

- connection-bytes, connection-mark, connection-type
- connection-state
- connection-limit
- connection-rate
- layer7-protocol
- new-connection-mark
- tarpit



# Firewall Connection Tracking

❖ Status koneksi pada **connection tracking** :

- **New** : Membuka koneksi baru
- **Established** : Memiliki koneksi yang sudah dikenal
- **Related** : Paket membuka koneksi baru tetapi memiliki hubungan dengan koneksi yang sudah diketahui
- **Invalid** : Paket tidak termasuk koneksi yang diketahui.





# Praktikum Firewall



Organized By : Politeknik Astra



# Topologi Praktikum Firewall Dasar



## **WIFI STATION INFORMATION**

WLAN1 : MODE STATION  
DHCP CLIENT : ENABLE  
SSID : STUDENT POLTEK ASTRA  
PASSWORD : PoltekAstra@2021  
NAT : MASQUARADE



**IP Ether 1 : 172.16.200.254/24**



**IP LAPTOP : 172.16.200.1/24**

### ❖ Implementasi Filter Rule

1. Izinkan hanya IP Laptop yang Dapat Mengakses MikroTik
2. Blok Koneksi Internet Berdasarkan IP Address
3. Blok Situs Internet Dengan Content
4. Blok Situs Internet Dengan Dst Address
5. Blok Situs Internet Dengan TLS-HOST
6. Blok Situs Internet Dengan Layer 7 Protocol

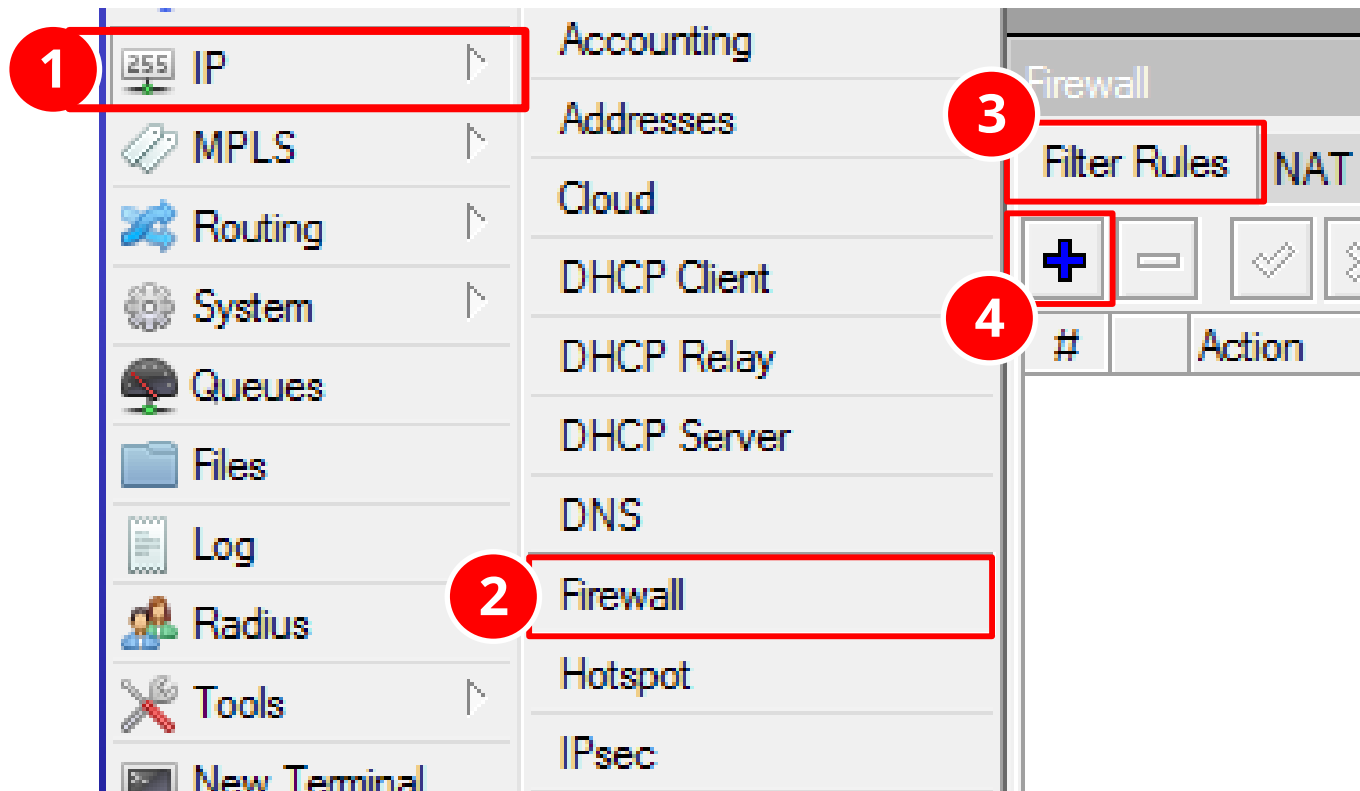
### ❖ Implementasi Address List

1. Address List Untuk Blok Client Berdasarkan Grup
2. Address List Untuk Blok Internet Berdasarkan Nama Domain

## Izinkan hanya IP Laptop yang Dapat Mengakses MikroTik

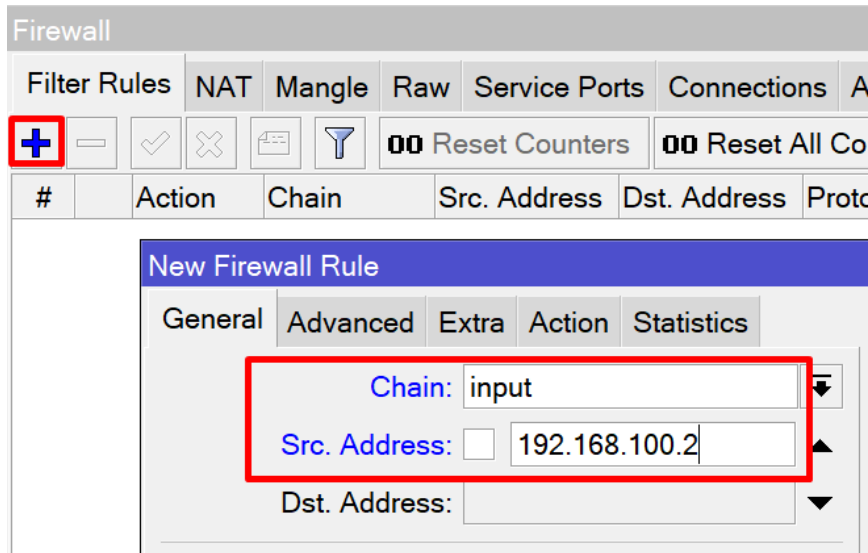
Untuk melakukan blok client berdasarkan IP Address ,

Klik **IP - Firewall - Filter Rule** – klik **Add [+]**.



# Izinkan hanya IP Laptop yang Dapat Mengakses MikroTik

IF ada traffic **input** yang berasal dari IP laptop (**192.168.100.2**)



The screenshot shows the Mikrotik WinBox Firewall Filter Rule configuration window. The 'Filter Rules' tab is selected. A red box highlights the '+' button in the top left corner. Below the table, the 'New Firewall Rule' dialog is open, showing the 'General' tab. The 'Chain' is set to 'input', and the 'Src. Address' is set to '192.168.100.2'. The 'Dst. Address' is empty.

#	Action	Chain	Src. Address	Dst. Address	Prot
---	--------	-------	--------------	--------------	------

New Firewall Rule

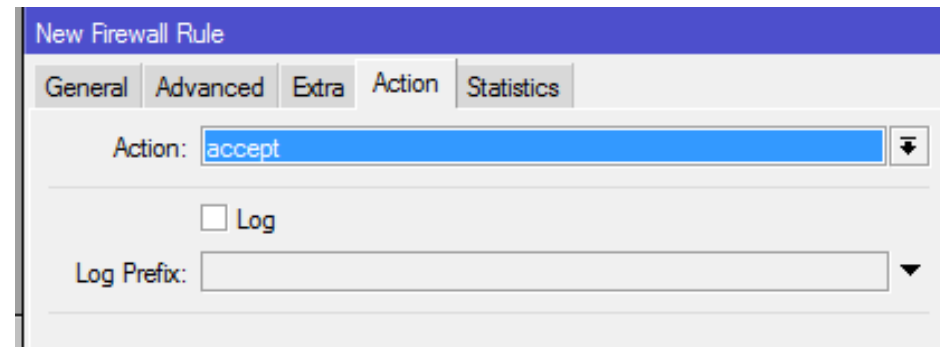
General Advanced Extra Action Statistics

Chain: input

Src. Address: 192.168.100.2

Dst. Address:

THEN tentukan action > **accept**



The screenshot shows the Mikrotik WinBox Firewall Filter Rule configuration window, specifically the 'Action' tab. The 'Action' is set to 'accept'. The 'Log' checkbox is unchecked, and the 'Log Prefix' is empty.

New Firewall Rule

General Advanced Extra Action Statistics

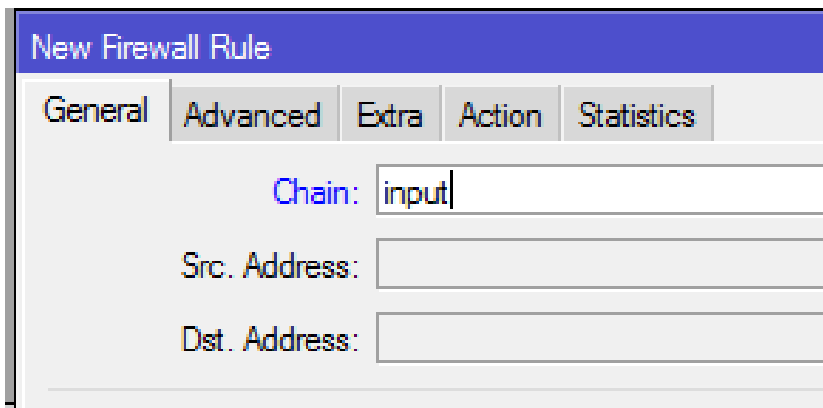
Action: accept

☐ Log

Log Prefix:

## Izinkan hanya IP Laptop yang Dapat Mengakses MikroTik

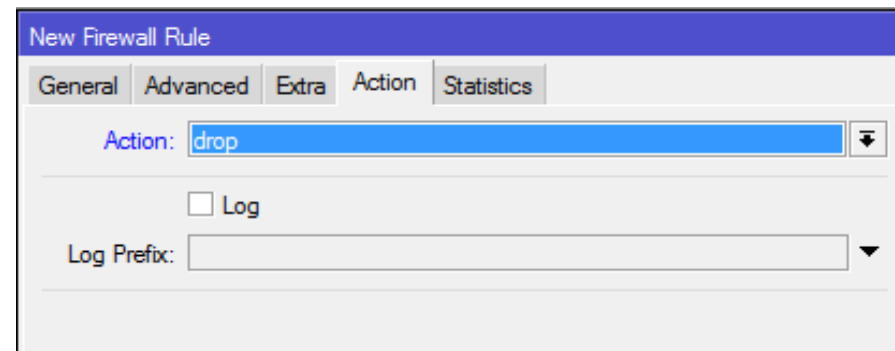
IF ada traffic **input** yang berasal dari <kosong> atau “any address/network”



The screenshot shows the 'New Firewall Rule' window with the 'General' tab selected. The 'Chain' field is set to 'input'. The 'Src. Address' and 'Dst. Address' fields are empty, indicating traffic from any source to any destination.

Field	Value
Chain	input
Src. Address	
Dst. Address	

THEN tentukan action > **drop**



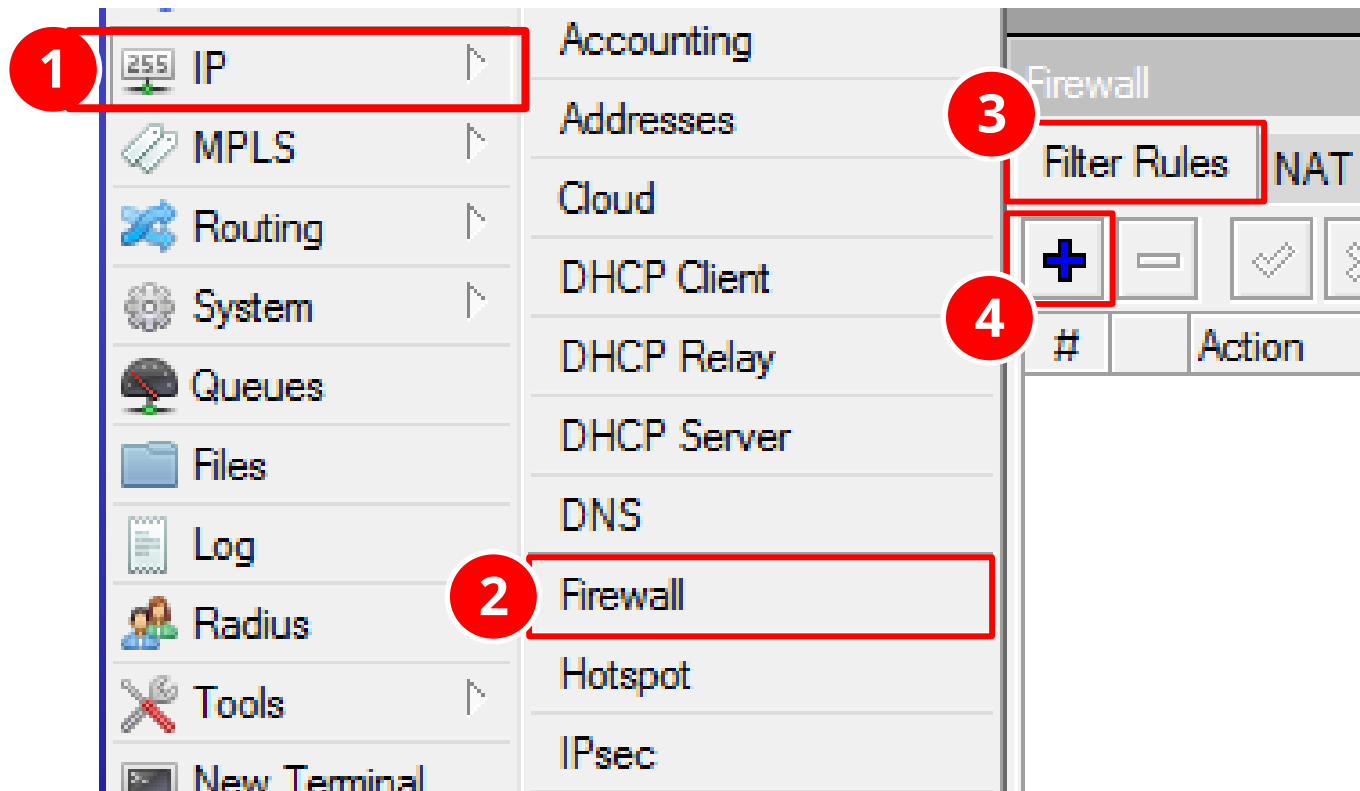
The screenshot shows the 'New Firewall Rule' window with the 'Action' tab selected. The 'Action' dropdown menu is set to 'drop'. The 'Log' checkbox is unchecked, and the 'Log Prefix' field is empty.

Field	Value
Action	drop
Log	<input type="checkbox"/>
Log Prefix	

# Blok Koneksi Internet Berdasarkan IP Address

Untuk melakukan blok client berdasarkan IP Address ,

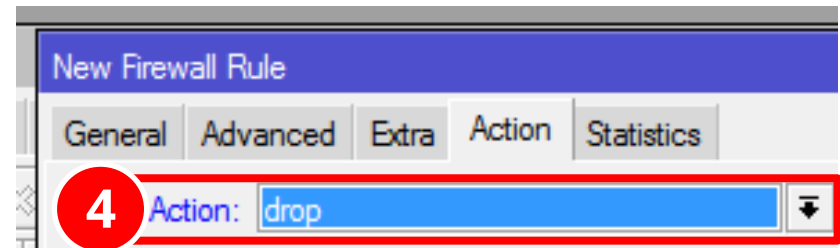
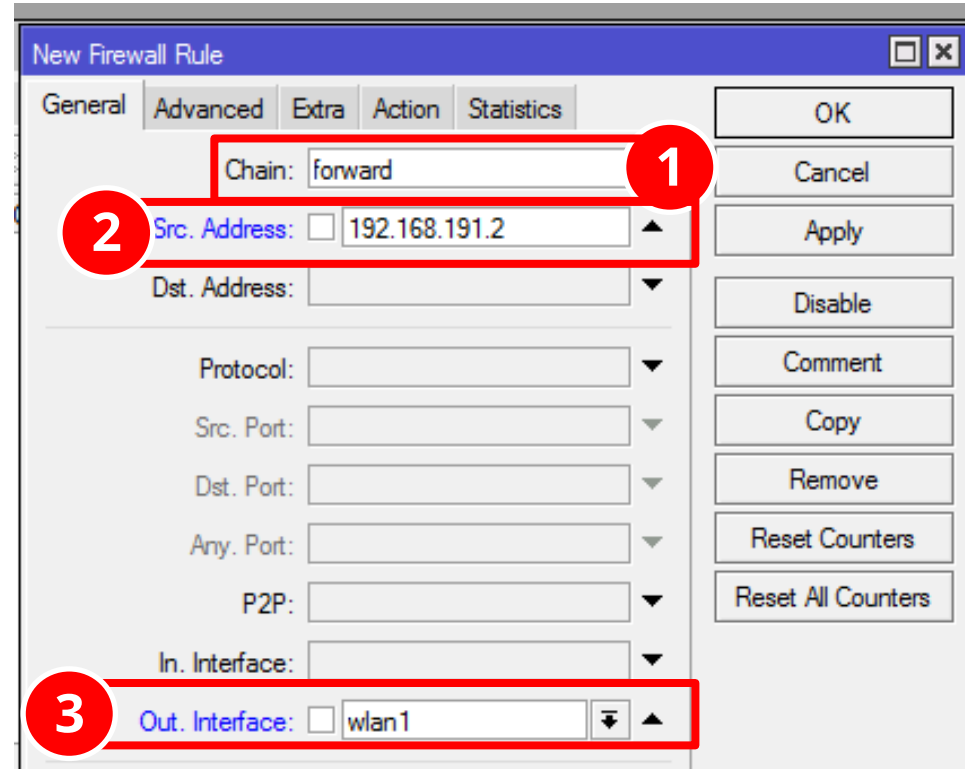
Klik **IP - Firewall - Filter Rule** – klik **Add [+]**.



# Blok Koneksi Internet Berdasarkan IP Address

Kemudian :

1. Isi **chain** dengan **forward** karena tujuannya adalah untuk memforwardkan paket dari lokal ke publik dan sebaliknya.
2. Masukkan **IP address PC client** yang akan diblock.
3. Gunakan **Wlan1** sebagai out interface. Lalu Ok.
4. Dan Pada Tab Action pilih **DROP** lalu OK





# Blok Situs Internet Dengan Content

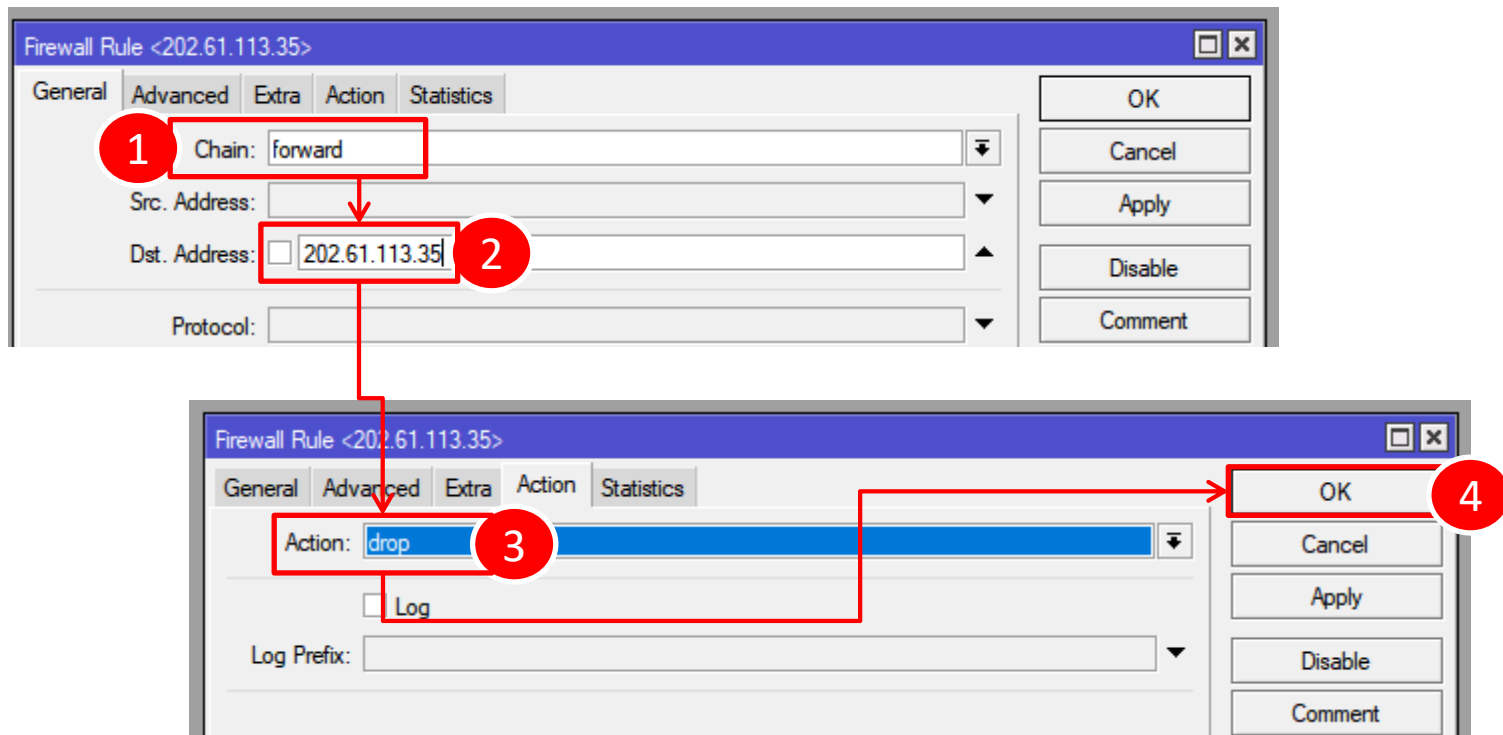
- ❖ Content merupakan string yang ditampilkan di halaman website. Misalnya kita ingin melakukan blok terhadap website atau situs tertentu misalnya facebook. maka website yang memiliki string yang kita isikan di parameter content akan difilter oleh firewall sehingga kita tidak bisa mengakses situs tersebut.

The image shows a sequence of steps in Mikrotik WinBox to configure a Firewall Rule. Red circles with numbers 1 through 8 indicate the sequence of actions:

1. Click on the **IP** menu in the left sidebar.
2. Click on the **Firewall** sub-menu.
3. Click the **+** button to add a new Firewall Rule.
4. In the **General** tab, set the **Chain** to **forward**.
5. In the **General** tab, set the **Out. Interface** to **wlan1**.
6. Click the **Advanced** tab.
7. In the **Advanced** tab, set the **Content** field to **facebook.com**.
8. In the **Action** tab, set the **Action** to **drop**.

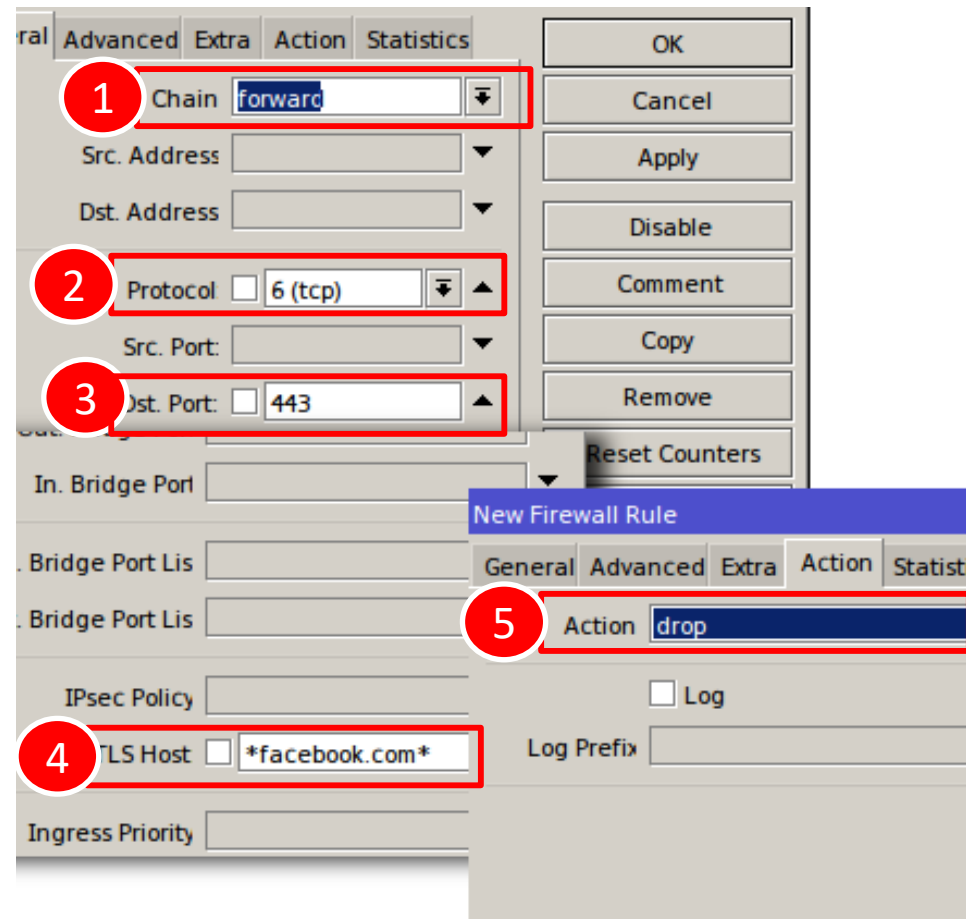
## Blok Situs Internet Dengan Dst Address

- ❖ Dst Address merupakan salah satu fitur yang bisa kita gunakan untuk melakukan blok sebuah website dimana kita cukup mengisi IP Address dari sebuah website tersebut.



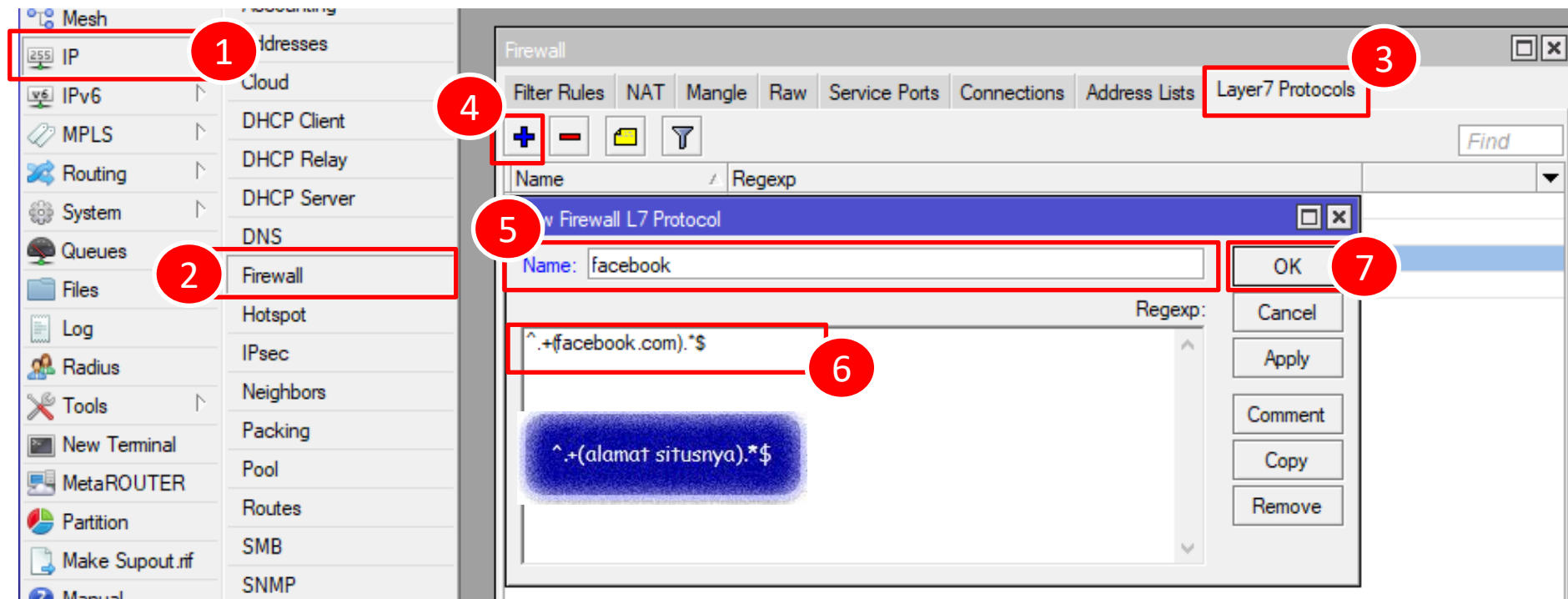
# Blok Situs Internet Dengan TLS-HOST

- ❖ MikroTik menambahkan sebuah parameter **TLS Host** mulai versi 6.41, pada menu IP Firewall dimana dengan parameter tersebut kita bisa dengan mudah melakukan filtering trafik HTTPS.
- ❖ Penambahan ini memang didasarkan pada banyaknya website yang sekarang ini menggunakan protokol HTTPS untuk komunikasinya.



# Blok Situs Internet Dengan Layer 7 Protocol

- ❖ Jika Anda familiar dengan regexp, Anda juga bisa menerapkan filtering pada layer7 menggunakan firewall filter. Di mikrotik, penambahan regexp bisa dilakukan di menu Layer 7 Protocol. Perlu diketahui bahwa penggunaan regexp, akan membutuhkan resource CPU yang lebih tinggi dari rule biasa.

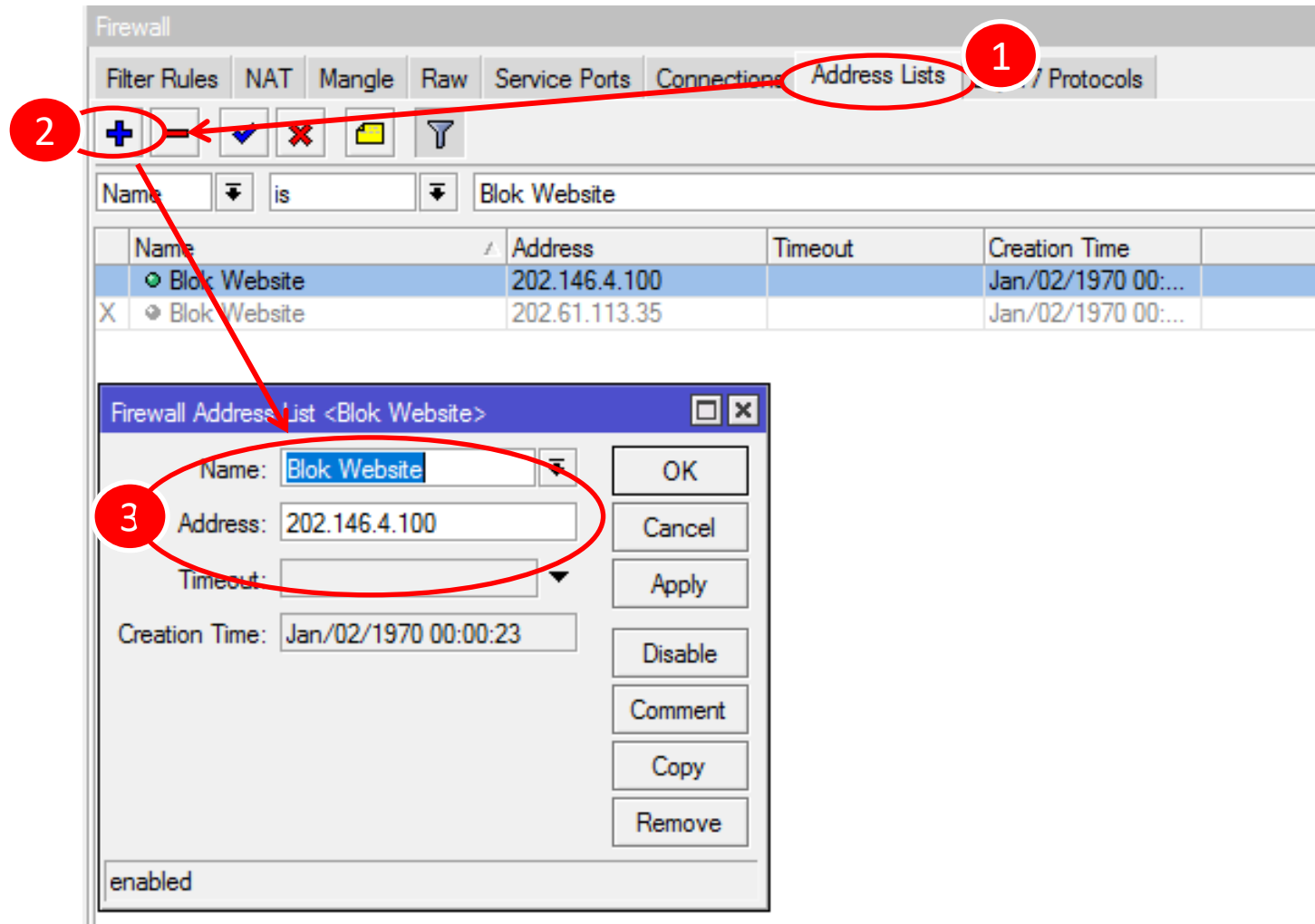




## Address List [1]

- ❖ Address-list digunakan untuk memfilter group IP address dengan 1 rule firewall.
- ❖ Address-list juga bisa merupakan hasil dari rule firewall dengan action “add to address list”
- ❖ Satu line address-list dapat berupa subnet, range, atau 1 host IP address

# Address List Untuk Blok Client Berdasarkan Grup [1]



# Address List – Dynamic Domain

The screenshot shows the Mikrotik WinBox Firewall configuration interface. The 'Address Lists' tab is selected, indicated by a red circle and the number 1. Below the tabs, a toolbar contains a '+' icon for adding a new list, which is circled with a red circle and the number 2. A red arrow points from this icon to a dialog box titled 'Firewall Address List <Sosmed>'. In this dialog box, the 'Name' field is set to 'Sosmed', which is circled with a red circle and the number 3. The 'Address' field is set to 'www.kompas.com'. Other fields include 'Timeout' and 'Creation Time'. The dialog box also has buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. At the bottom of the dialog box, it says 'enabled'.

Name	Address	Timeout	Creation Time
Sosmed	www.kompas.com		Apr/14/2017 06:5...
... www.kompas.com			
D Sosmed	192.168.200.1		Apr/14/2017 06:5...



# TERIMA KASIH



**Organized By : Politeknik Astra**