

**BAB 2**

**FIREWALL**

## **Fungsi Firewall (Overview)**

Firewall digunakan untuk membatasi akses antara dua jaringan yang saling terhubung, yaitu antara jaringan internal dengan jaringan global (internet). Firewall diletakkan diantara kedua jaringan internal dan global, sehingga semua informasi yang keluar maupun masuk harus melewati firewall. Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewat atau tidak, antara lain Alamat IP dari komputer sumber:

- Alamat IP dari komputer tujuan.

- Port TCP/UDP sumber dari sumber.

- Port TCP/UDP tujuan data pada komputer tujuan.

- Informasi dari header yang disimpan dalam paket data.

Tujuan utama firewall adalah menjaga agar akses internal maupun eksternal dari orang yang tidak berwenang atau tidak mempunyai akses. Firewall merupakan suatu cara yang efektif untuk melindungi jaringan dari ancaman gangguan lewat internet. Membatasi dan menjaga kerusakan pada satu bagian jaringan agar tidak menyebar ke bagian yang lain pada jaringan.

## **Manfaat Firewall**

Berikut ini beberapa manfaat apabila dalam pemasangan jaringan menggunakan firewall:

- Seluruh akses dalam jaringan dapat kita kontrol melalui firewall.

- Dapat menjaga informasi rahasia berharga yang menyali keluar tanpa sepengetahuan.

- Dapat mengawasi semua service berjalan.

- Dapat mencatat dan merekam semua kegiatan berjalan melewatinya.

- Dapat menerapkan suatu kebijakan keamanan (Security Policy).

- Dapat mencegah suatu paket yang dirasa mencurigkan oleh sistem.

- Dapat menghambat pergerakan para penyerang yang mencoba memasuki sistem.

## **Cara Kerja Firewall**

Komputer memiliki ribuan port yang dapat diakses untuk berbagai keperluan. Cara Kerja Firewall dari komputer adalah menutup port kecuali untuk beberapa port tertentu yang perlu tetap terbuka. Firewall di komputer bertindak sebagai garis pertahanan terdepan dalam mencegah semua jenis hacking ke dalam jaringan, karena, setiap hacker yang mencoba untuk menembus ke dalam jaringan komputer akan mencari port yang terbuka yang dapat diaksesnya.

Dalam Jaringan firewall terdapat dua buah cara yang dapat kita gunakan agar komunikasi jaringan dapat berjalan sesuai dengan fungsinya, yaitu menggunakan **packet filtering** dan **sistem proxy**, berikut penjelasnya.

### **Packet Filtering**

Packet filtering biasa juga disebut dengan screening router, yaitu suatu router yang melakukan routing paket antara jaringan internal dan jaringan eksternal sesuai dengan kebijakan keamanan yang digunakan pada suatu jaringan. Dengan kata lain, packet filtering hanya dapat dipakai untuk menyaring paket-paket yang digunakan dengan paket-paket yang tidak digunakan dan mempunyai resiko keamanan yang lebih besar. Informasi yang digunakan untuk menyaring paket-paket antara lain alamat IP address asal dan tujuannya, Protokol yang digunakan (TCP, UDP, atau ICMP), dan alamat port asal dan tujuannya.

### **Sistem Proxy**

Proxy merupakan suatu program server atau aplikasi spesifik yang dijalankan pada mesin firewall. Setiap komunikasi yang terjadi antara dua buah jaringan dilakukan melalui suatu operator (Proxy Server). Firewall akan menggunakan kombinasi antara packet filtering dan sistem proxy, karena tidak semua kinerja protokol jaringan dapat berjalan secara maksimal sesuai dengan salah satu dari kedua teknik tersebut.

Proxy dalam melakukan tugasnya mengambil user request untuk internet service seperti HTTP, FTP dan meneruskannya pada host yang menjadi tujuannya. Dapat disimpulkan,

proxy merupakan perantara antara jaringan internal dengan jaringan global (internet).

## Cara Kerja Firewall Filter Rule

### Prinsip IF....THEN....

- IF (jika) packet memenuhi syarat kriteria yang kita buat.
- THEN (maka) action apa yang akan dilakukan pada packet tersebut

#### IF (Jika)

New Firewall Rule

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Source IP (IP client)

Destination IP (IP internet)

Protocol (TCP/UDP/ICMP, dll)

Source port (biasanya port dari client)

Destination port (service port tujuan)

Interface (traffik masuk atau keluar)

Paket yang sebelumnya telah ditandai

#### THEN (maka)

New Firewall Rule

General Advanced Extra Action Statistics

Action:

Log Prefix:

accept

add dst to address list

add src to address list

drop

fasttrack connection

jump

log

passthrough

reject

return

tarpit

**accept** - accept the packet. Packet is not passed to next firewall rule.

**add-dst-to-address-list** - add destination address to [address list](#) specified by address-list parameter

**add-src-to-address-list** - add source address to [address list](#) specified by address-list parameter

**drop** - silently drop the packet

**jump** - jump to the user defined chain specified by the value of jump-target parameter

**log** - add a message to the system log containing following data: in-interface, out-interface, src-mac, protocol, src-ip:port->dst-ip:port and length of the packet. After packet is matched it is passed to next rule in the list, similar as passthrough

**passthrough** - ignore this rule and go to next one (useful for statistics).

**reject** - drop the packet and send an ICMP reject message

**return** - passes control back to the chain from where the jump took place

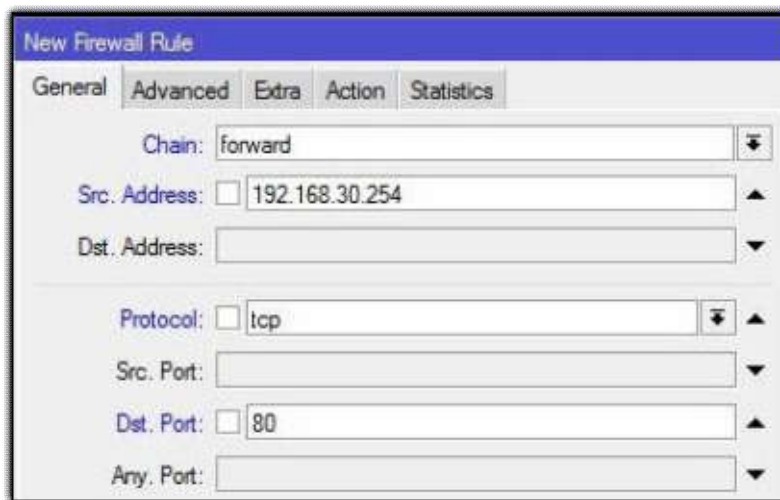
**tarpit** - captures and holds TCP connections (replies with SYN/ACK to the inbound TCP SYN packet)

Selanjutnya saya akan Sedikit menjelaskan Parameter Parameter yang bisa kita gunakan

di Firewall

### Protokol dan Port

Penggunaan port dan protokol ini biasa di kombinasikan dengan IP address. Misalkan Anda ingin client tidak bisa browsing, namun masih bisa FTP, maka Anda bisa buat rule firewall yang melakukan blok di protokol TCP port 80. Ketika Anda klik tanda drop down pada bagian protokol, maka akan muncul opsi protokol apa saja yang akan kita filter. Parameter ini akan kita butuhkan ketika kita ingin melakukan blok terhadap aplikasi dimana aplikasi tersebut menggunakan protokol dan port yang spesifik.



### Interface

Interface secara garis besar ada 2, input interface dan output interface. Cara menentukannya adalah dengan memperhatikan dari interface mana trafik tersebut masuk ke router, dan dari interface mana trafik tersebut keluar meninggalkan router. Misalkan Anda terkoneksi ke internet melalui router mikrotik, kemudian Anda ping ke [www.mikrotik.co.id](http://www.mikrotik.co.id) dari laptop Anda, maka input interface adalah interface yang terkoneksi ke laptop Anda, dan output interface adalah interface yang terkoneksi ke internet. Contoh penerapannya adalah ketika Anda ingin menjaga keamanan router, Anda tidak ingin router bisa diakses dari internet. Dari kasus tersebut Anda bisa lakukan filter terhadap koneksi yang masuk ke router dengan mengarahkan opsi in-interface pada interface yang terkoneksi ke internet.



In. Interface:

Out. Interface:

### Parameter P2P

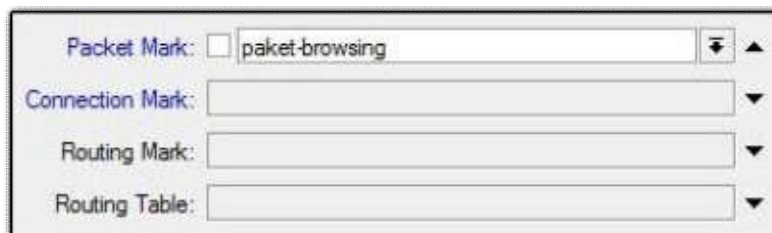
Sebenarnya ada cara yang cukup mudah dan simple untuk melakukan filtering terhadap traffick P2P seperti torrent atau edonkey. Jika sebelumnya Anda menggunakan banyak rule, Anda bisa sederhanakan dengan menentukan parameter P2P pada rule firewall filter. Jika Anda klik bagian drop down, akan muncul informasi program p2p yang dapat di filter oleh firewall.



P2P:

### Mangle

Kita biasanya membuat mangle untuk menandai paket/koneksi, kemudian kita gunakan untuk bandwidth management. Akan tetapi kita juga bisa membuat mangle untuk melakukan filtering. Firewall filter tidak dapat melakukan penandaan pada paket atau koneksi, akan tetapi kita bisa kombinasikan mangle dan firewall filter. Pertama, kita tandai terlebih dahulu paket atau koneksi dengan mangle, kemudian kita definisikan di firewall filter dan fitur yang lainnya.



Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

### ConnectionState

Jika Anda tidak ingin ada paket - paket invalid lalu lalang di jaringan Anda, Anda juga bisa melakukan filtering dengan mendefinisikan parameter connection state. Paket invalid merupakan paket yang tidak memiliki koneksi dan tidak berguna sehingga hanya akan membebani resource jaringan. Kita bisa melakukan drop terhadap paket - paket ini dengan mendefinisikan parameter connection state.

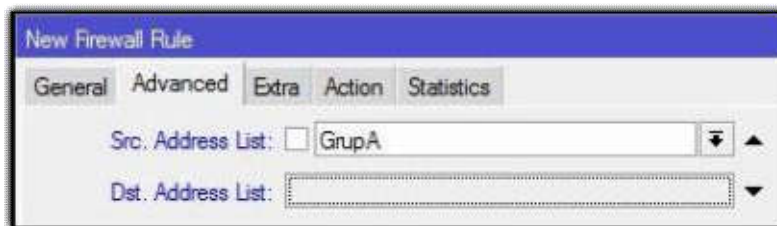


Connection Type:

Connection State:

### Address List

Ada saat dimana kita ingin melakukan filtering terhadap beberapa ip yang tidak berurutan atau acak. Apabila kita buat rule satu per satu, tentu akan menjadi hal yang melelahkan. Dengan kondisi seperti ini, kita bisa menerapkan grouping IP membuat "address list". Pertama, buat daftar ip di address list, kemudian terapkan di filter rule Anda. Opsi untuk menambahkan parameter "Address List" di firewall ada di tab Advanced. Ada 2 tipe address list, "Src. Address List" dan "Dst. Address List. Src Address List adalah daftar sumber ip yang melakukan koneksi, Dst Address List adalah ip tujuan yang hendak diakses.



### 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. Setelah Anda menambahkan regexp, Anda bisa melakukan filtering dengan mendefinisikan Layer 7 Protocol pada rule filter yang Anda buat. Perlu diketahui bahwa penggunaan regexp, akan membutuhkan resource CPU yang lebih tinggi dari rule biasa.



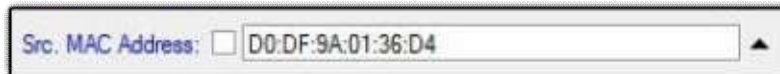
### Content

Saat kita hendak melakukan blok terhadap website, salah satu langkah yang cukup mudah untuk melakukan hal tersebut adalah dengan melakukan filter berdasarkan content. Content merupakan string yang tertampil di halaman website. Dengan begitu, website yang memiliki string yang kita isikan di content akan terfilter oleh firewall. Misalkan kita ingin block www.facebook.com maka cukup isi parameter content dengan string "facebook" dan action drop, maka website facebook baik HTTP maupun HTTPS tidak dapat diakses.



## Mac address

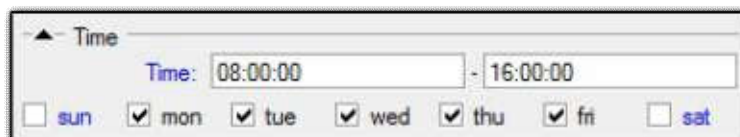
Ketika kita melakukan filter by ip address, terkadang ada user yang nakal dengan mengganti ip address. Untuk mengatasi kenakalan ini, kita bisa menerapkan filtering by mac-address. Kita catat informasi mac address yang digunakan user tersebut, kemudian kita tambahkan parameter Src. Mac Address di rule firewall kita. Dengan begitu selama user tersebut masih menggunakan device yang sama, dia tetap ter-filter walaupun berganti ip.



## Time

Salah satu solusi alternatif selain kita harus repot membuat scheduler dan script, kita bisa memanfaatkan fitur time di firewall filter. Fitur ini akan menentukan kapan rule firewall tersebut dijalankan. Bukan hanya untuk menentukan jam saja, fitur ini juga bisa digunakan untuk menentukan hari apa saja rule tersebut berjalan. Misalkan kita ingin melakukan block facebook di jam kerja, maka kita bisa buat rule firewall yang melakukan block facebook yang dijalankan dari jam 08:00 sampai jam 16:00 selain hari Sabtu dan Minggu.

Sebelum anda membuat rule firewall dengan parameter "time", pastikan Anda sudah set NTP di router Anda agar waktu router sesuai dengan waktu real.



Saat Anda membuat rule firewall, usahakan untuk membuat rule yang spesifik. Semakin spesifik rule yang kita buat, maka semakin optimal pula rule tersebut akan berjalan.



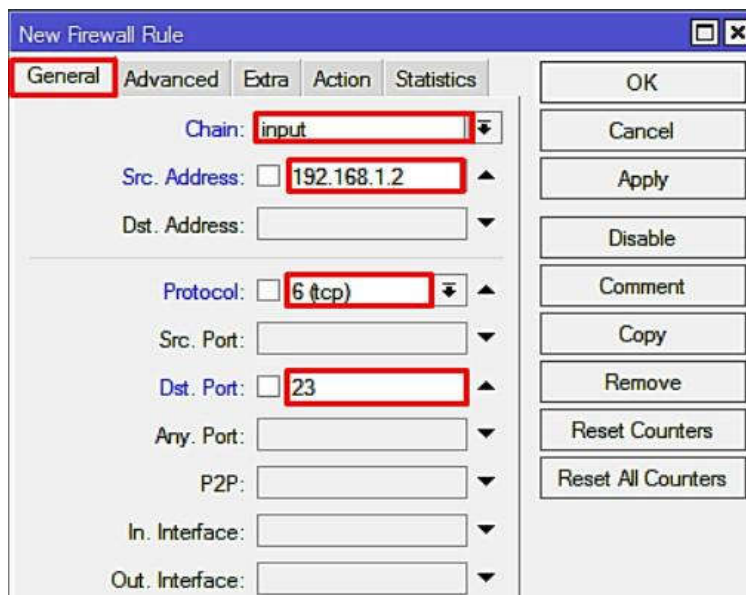
## LAB 12 Melindungi Router dengan Filter Rule

Di lab ini kita akan membahas bagaimana cara melindungi Router dengan Filter Rule, fungsi Filter rule di sini adalah Membuat izin akses masuk ke Router, di lab ini kita akan mencoba membuat Rule agar IP 192.168.1.2 bisa melakukan akses telnet ke router dan selain IP 192.168.1.2 tidak bisa akses telnet ke router

Pertama kita akan mencoba cara Accept few and Drop Any, yang artinya Terima beberapa dan Tolak Semua..

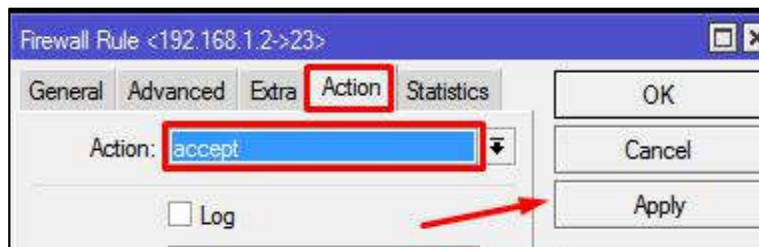
Klik IP > Firewall > Filter Rule > Add (+)

Isi Chain=Input,Src.Address=192.168.1.2 (IP PC),Protocol=TCP  
, Dst. Port=23 (Port Telnet)



Dan Pilih Action=Accept

Lalu Apply dan OK

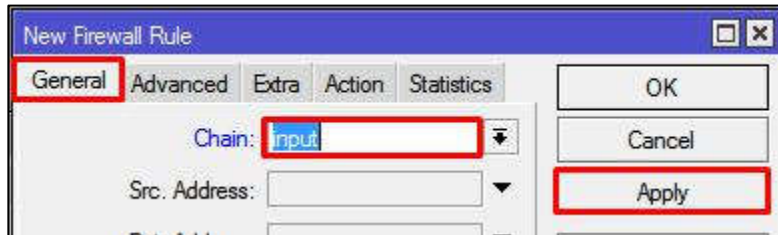


Jika Kita sudah Membuat Rule seperti itu maka Artinya "Jika ada yang masuk dengan IP 192.168.1.2 menggunakan Protocol TCP port 23 di perbolehkan"

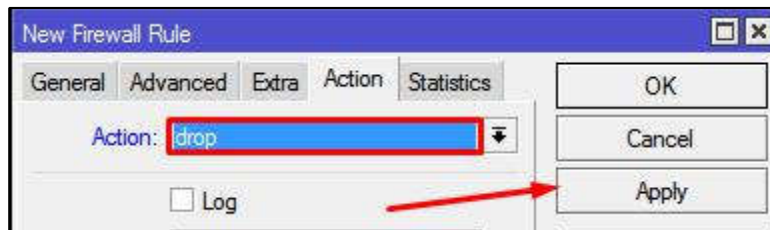
Selanjutnya adalah membuat Rule untuk menolak semua semua akses yang masuk ke router...

Klik IP > Firewall > Filter Rule > Add (+)

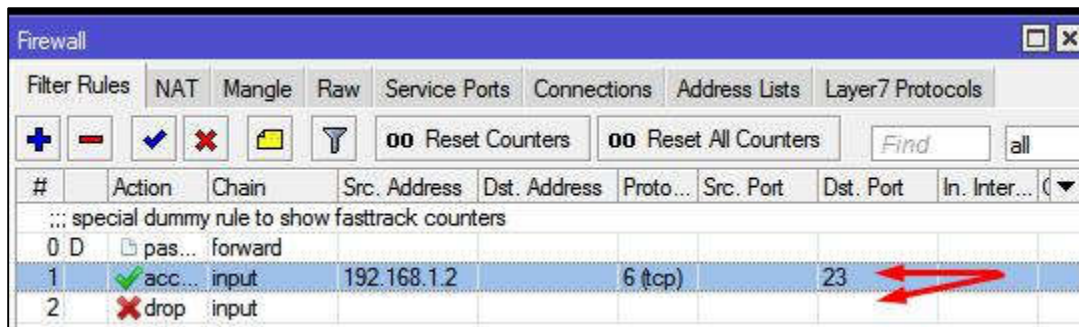
Isi Chain=Input



- Dan isi action=Drop
- Lalu Apply dan OK



Rule



Untuk pengetesan coba setting IP PC=192.168.1.2 jika kita menggunakan Ip tersebut maka kita tetap bisa meng-akses telnet ke Router,Tetapi jika kita menggunakan IP lain maka kita tidak bisa meng-Akses Router lewat telnet..

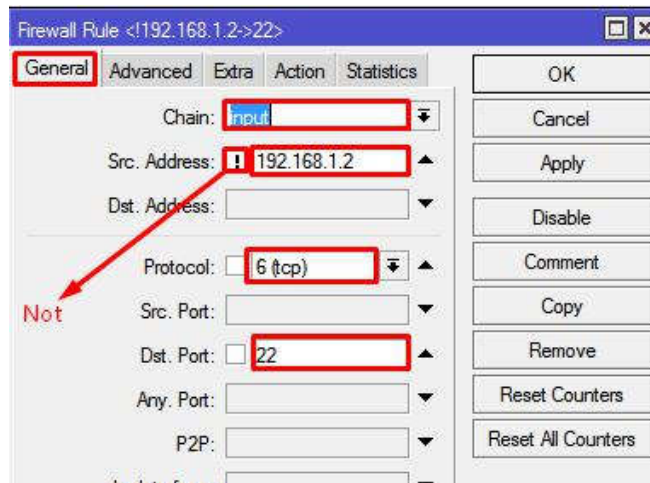
```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\420>telnet 192.168.1.1
Connecting To 192.168.1.1...Could not open connection to the host, on port 23: Connect failed
```

Ada cara yang lebih mudah dari Accept few and Drop any.....

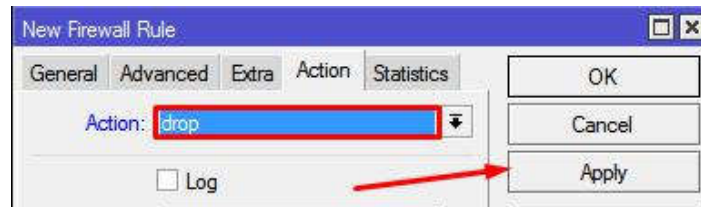
Klik IP > Firewall > Filter Rule > Add (+)

Isi Chain=Input ,Src.Adreess=(Not)192.168.1.2 (IP PC),Protocol=TCP  
,Dst.Port=23 (Port Telnet)



Kita harus meng-Klik fitur Not (  )

- Dan isi action=Drop
- Lalu Apply dan OK



Jika sudah membuat Rule tersebut maka artinya"jika ada yang masuk selain IP 192.168.1.2 maka akan di tolak"

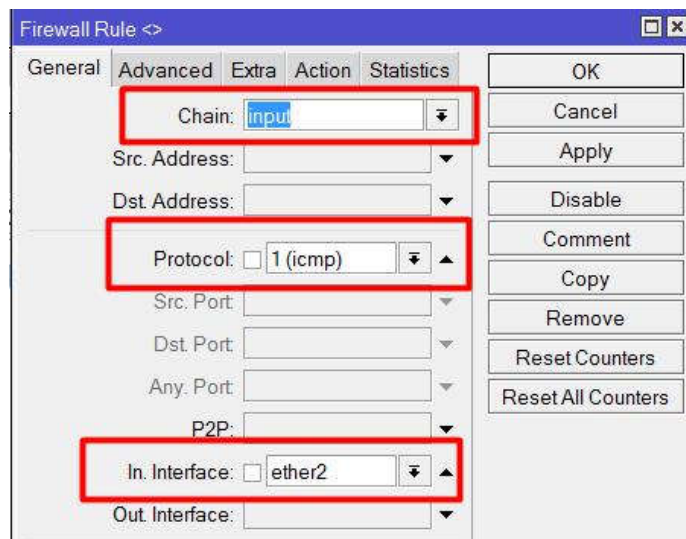
## LAB 13 Firewall Logging

Firewall logging adalah fitur yang ada pada firewall yang berfungsi untuk mencatat semua aktifitas jaringan di router kita yang akan di tampilkan di menu **log**, dengan ada nya fitur firewall logging kita dapat lebih mudah memantau aktifitas yang terjadi pada router kita, seperti contoh apabila ada yang **ping, telnet, ssh**, dan lain sebagainya, lalu bagaimana kah cara nya..??

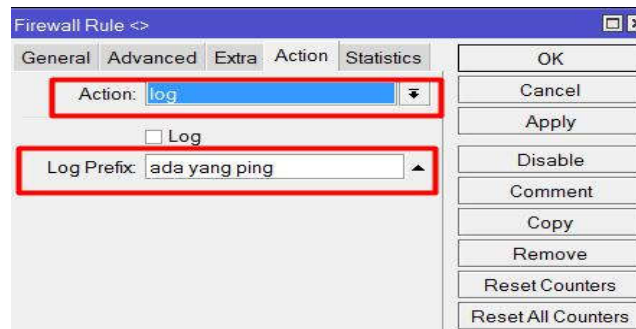
### Step by step :

Kita akan membuat rule logging untuk ping

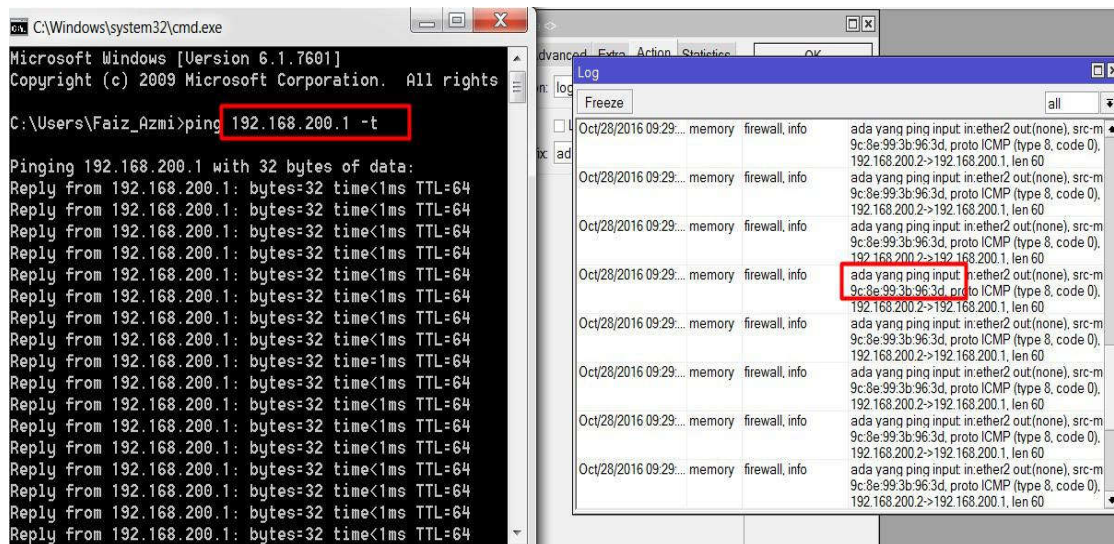
1. pasang terlebih dahulu IP di router kita (dapat di baca di lab yang sebelum nya )
2. pasang rule log di IP>firewall>filter rule>add(+)
3. lalu masukan **chain:input**, **protocol:icmp**(icmp merupakan prortocol untuk ping ), **in.interface=ether2**(port yang terhubung ke PC/laptop kita )



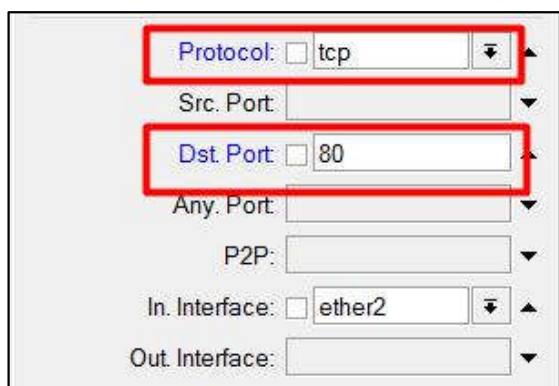
4. lalu masuk tab action dengan **action=log** dan **log.prefix=ada yang ping(hanya sekedar contoh)**



untuk pengecekan kita bisa langsung saja cek degna ping melalui CMD(command-line) ke IP router kita, dan setelah itu coba kita lihat di menu **log** apakah tercatat...???



Dan dalam firewall logging kita tidak hanya bisa membuat log untuk ping saja tetapi kita juga dapat membuat logging untuk ssh, telnet, webfig, bahkan winbox pun bisa...tetapi degan catatan kita harus sesuaikan degan dst.port dan protocol nya . seperti contoh webfig degan **protocol=tcp** dan **dst.port=80**



**Protocol dan port:**

1. Webfig: tcp 80
2. telnet: tcp 23
3. ping: icmp
4. Winbox: tcp 8291
5. ssh : 22

## LAB 14 Blok Situs dengan Filter Rule

Selain untuk melindungi router atau membuat log, firewall pun juga bisa memblock situs yang tidak diinginkan atau dalam kata lain di saat client ingin membuka situs melalui router kita firewall dalam router kita pun bisa untuk membentengi dari situs-situs yang tidak dibolehkan oleh server nya,

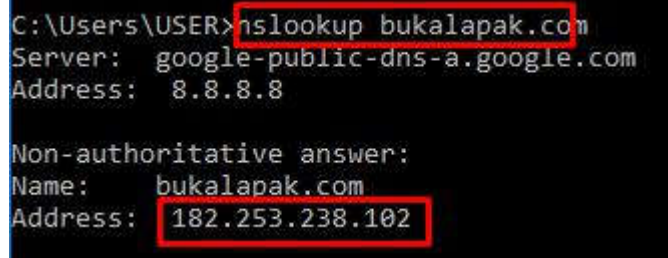
Dan dalam memblock situs ini kita memerlukan IP dari situs itu sendiri dan IP di sebuah situs itu terbagi menjadi 2:

1. **Single IP** : hanya ada satu IP
2. **Multiple IP** : memiliki satu atau lebih ip dalam satu situs

Cara melihat IP tersebut hanya dengan membuka CMD lalu ketik nslookup nama situs nya

Kita coba dahulu dengan memblock situs yang memiliki satu IP (**single IP**) **Step by step :**

1. Koneksikan laptop/PC kita ke internet melalui router seperti yang tertera di lab yang sebelum nya
2. Cari IP target situs melalui CMD (command-line) lalu ketik di CMD nslookup bukalapak.com (karna kita akan memblock situs kaskus) setelah itu tinggal enter saja dan dapat kita lihat IP yang tertera di situs tersebut

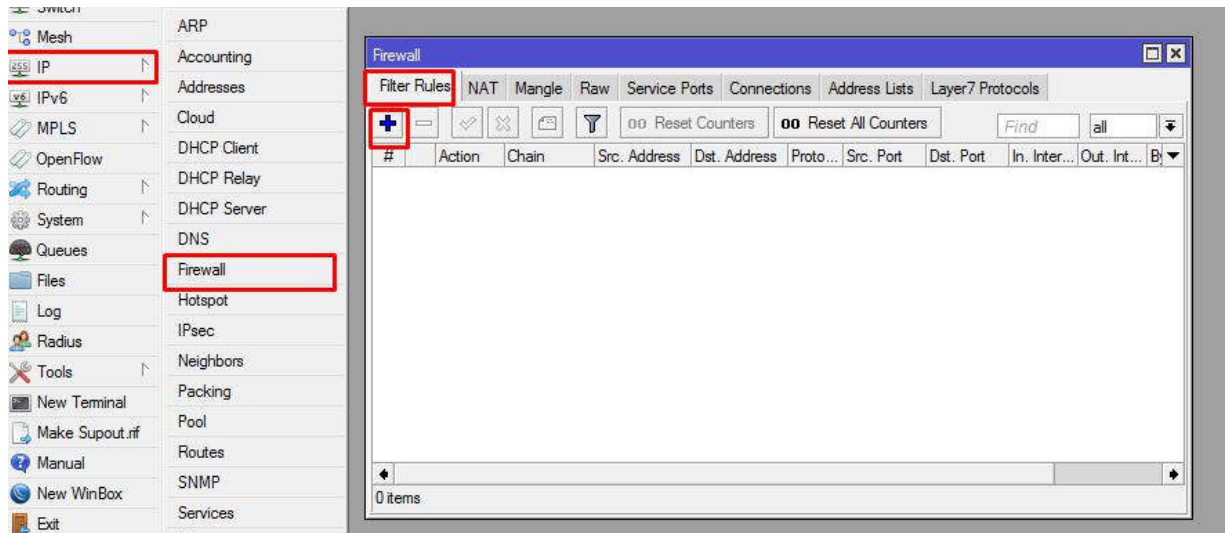


```
C:\Users\USER>nslookup bukalapak.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

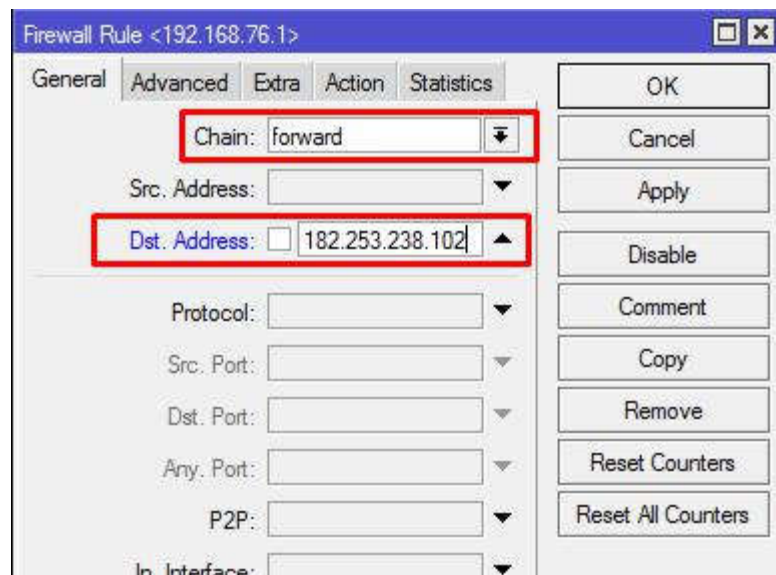
Non-authoritative answer:
Name:     bukalapak.com
Address:  182.253.238.102
```

3. Setelah itu kita tinggal masuk ke router kita
4. Cari menu IP>firewall>filter rules>add(+)

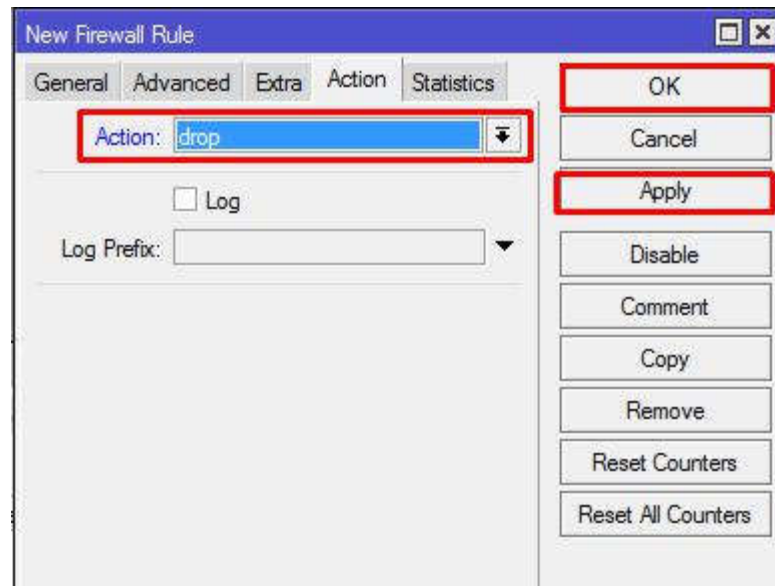




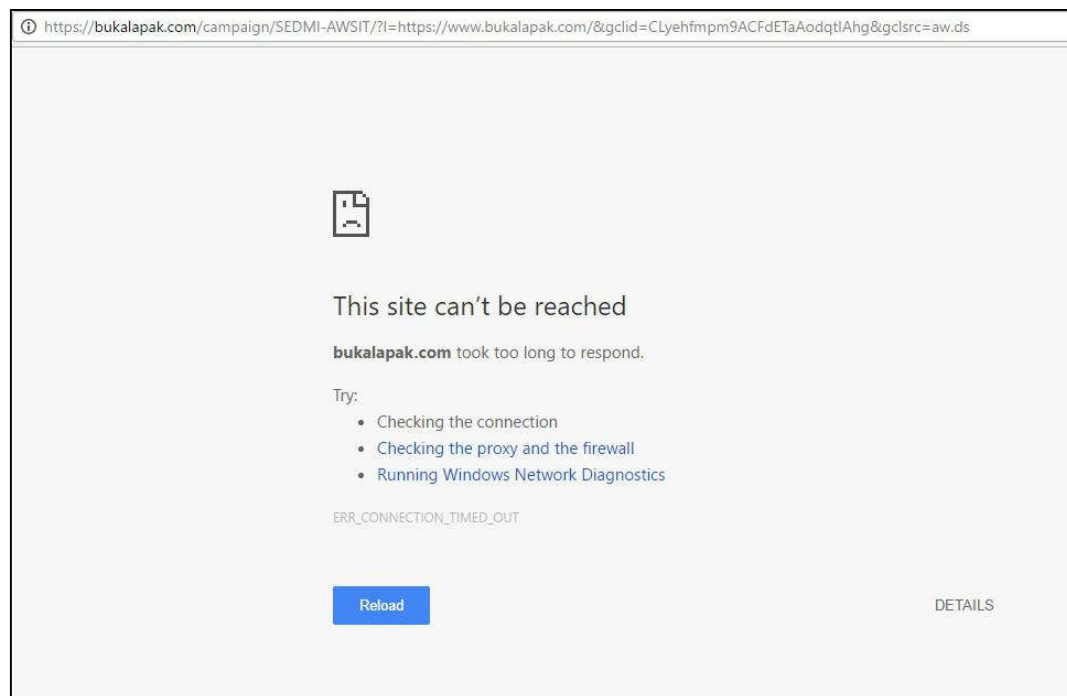
5. Lalu masukan **chain=forward**(karna kita akan memblock yang melewati router)  
**dst.address=182.253.238.102** (isikan IP situs yang tadi kita dapat kan/IP  
 bukalapak.com)



6. Masuk ke tab action dan isis-kan dengan **action=drop**(karna kita akan  
 menolak/memblock nya)



7. Dan untuk pengecekan kita dapat coba buka situs yang tadi kita block, apabila di browser tersebut hanya melooping/hanya berputar-putar saja lalu setelah itu akan muncul pesan error. itu tanda nya kita telah berhasil memblock situs tersebut



Yang baru saja kita lab adalah dari contoh **single IP** lalu bagaimanakah dengan **multiple IP**.....????

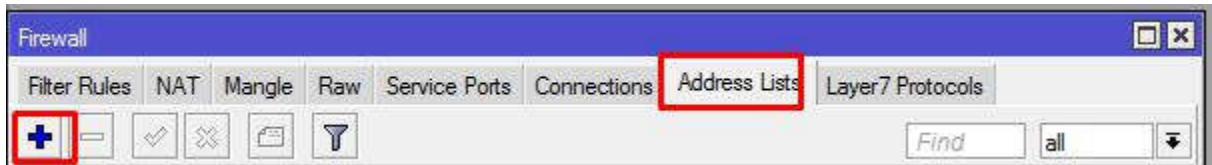
**Step by step :**

Kali ini kita akan memblock situs tokopedia.com dengan IP yang lebih dari satu (**multiple IP**)

1. Cara nya tidak jauh berbeda dengan **single IP** setelah kita koneksikan PC/laptop

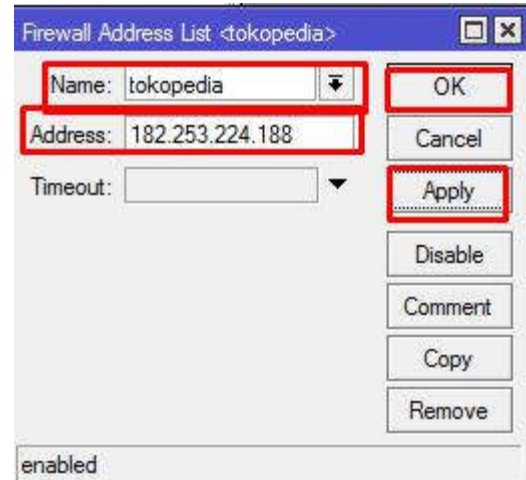
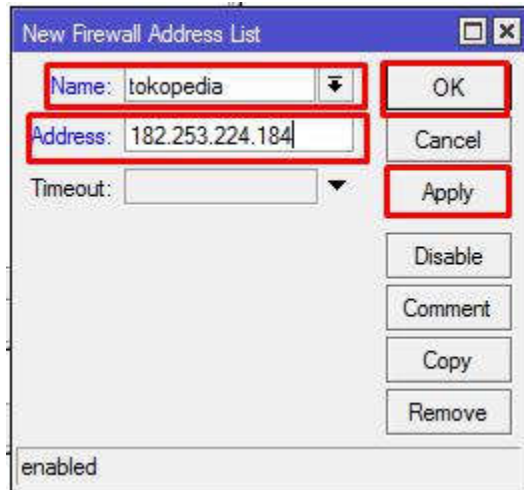


kita ke internet melalui router

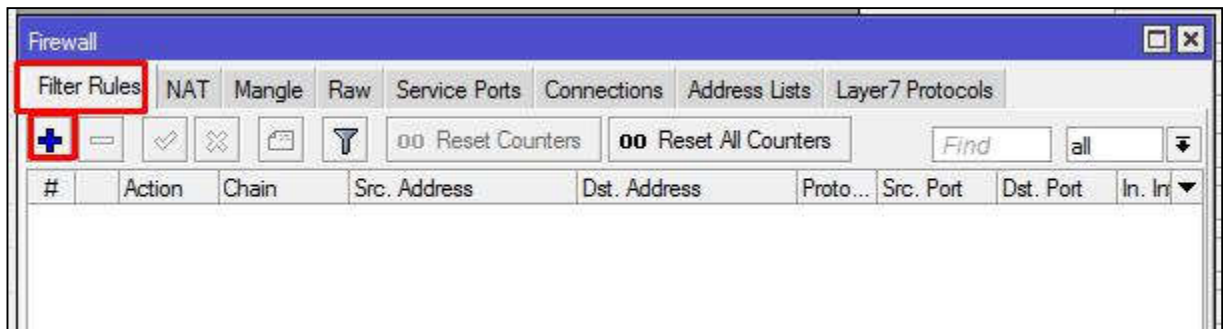
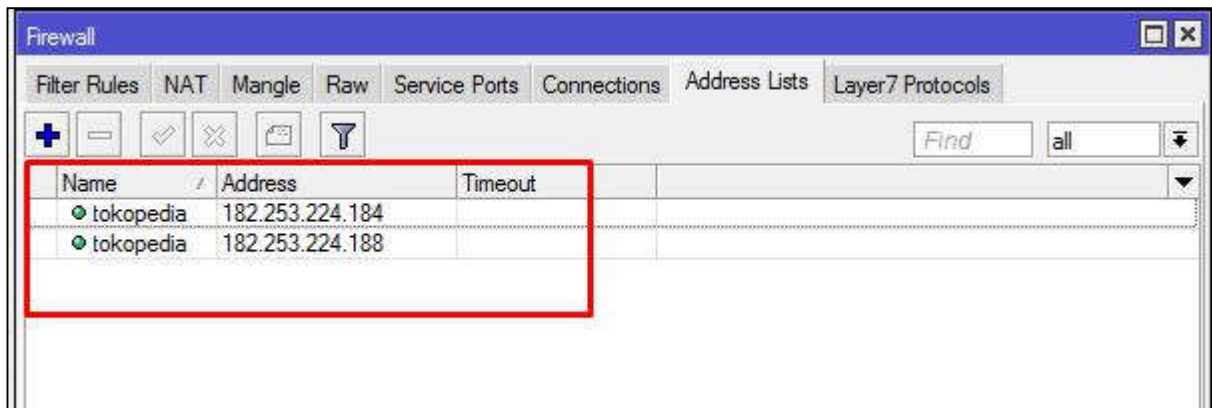


2. Masuk ke menu IP>firewall>address list>add(+)

3. masukan satu persatu IP situs yang tadi kita lihat dengan nama yang sama dan jangan lupa di apply dan ok

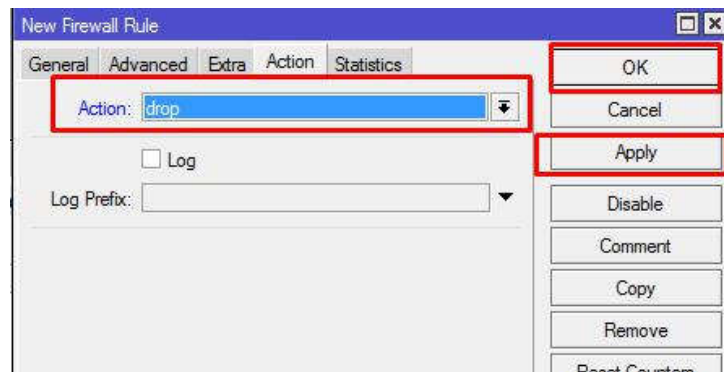
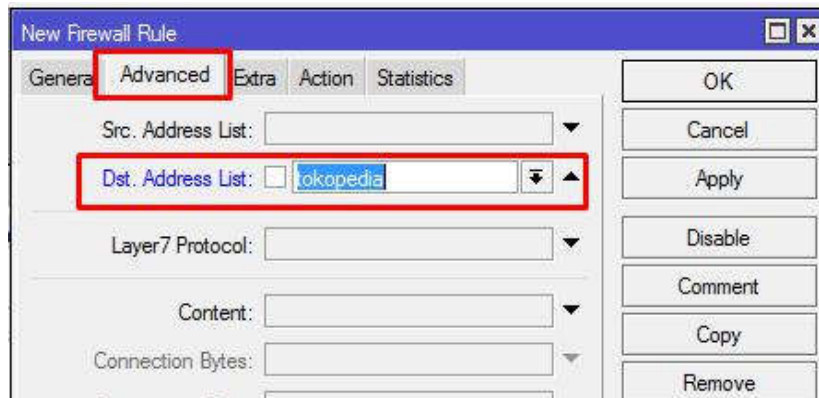
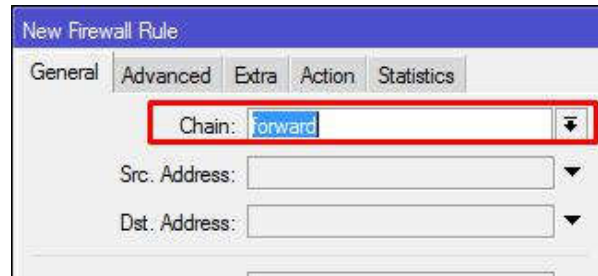


4. Maka setelah itu akan ada 2 address yang baru kita buat dengan nama yang sama



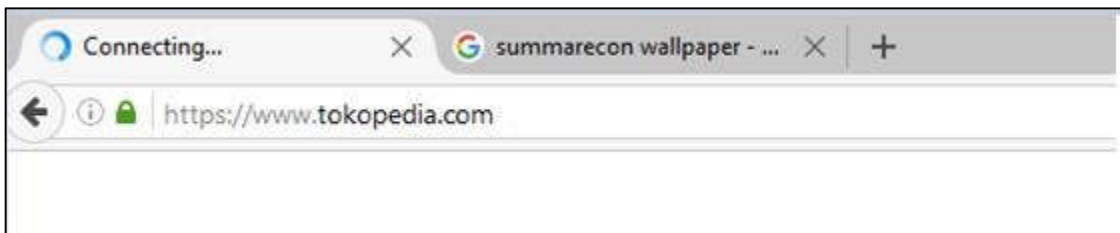
Setelah sudah, kita bisa langsung membuat rule di tab filter rules>add(+)

5. lalu masukan **chain=forward** masuk ke tab **advance** isikan di **dst.address list=bukalapak.com**(masukan address list yang tadi kita buat)



6. Lalu masuk ke tab action dengan **action=drop** dan di apply dan ok.

Dan untuk pengecekan nya sama seperti tadi hanya degan mengakases situs yang tadi kita drop apakah bisa atau tidak... maka nanti disaat kita buka maka ia akan terus melooping sampai nanti akan keluut pesan error, cukup mudah bukan...???



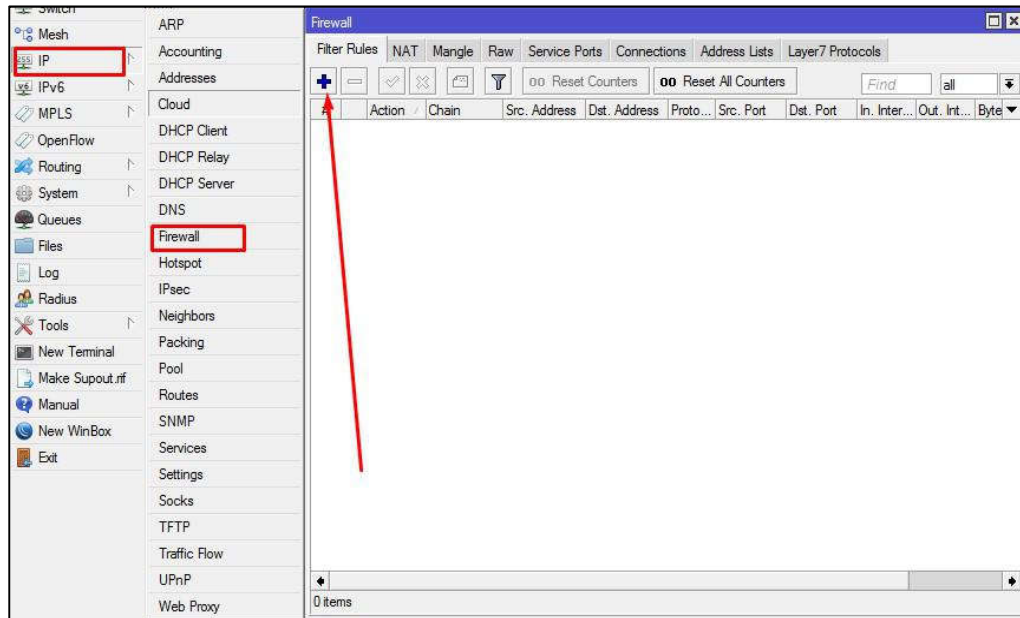
## LAB 15 Blok Konten

Pada suatu hari di desa yang sangat asri hiduplah seorang anak sekolah, umurnya kira-kira sekitar 16 tahun (kelas 2 SMK), sebut saja Jono. Jono ini orangnya pintar dan kreatif namun karena keterbatasan di bidang ekonomi ia tidak dapat mengapresiasi kepintarannya seperti mengikuti lomba-lomba atau olimpiade-olimpiade, jangankan lomba uang saku saja untung-untungan ia dapat. Di sekolah ia mengambil jurusan TKJ dan ia belajar tentang Mikrotik.

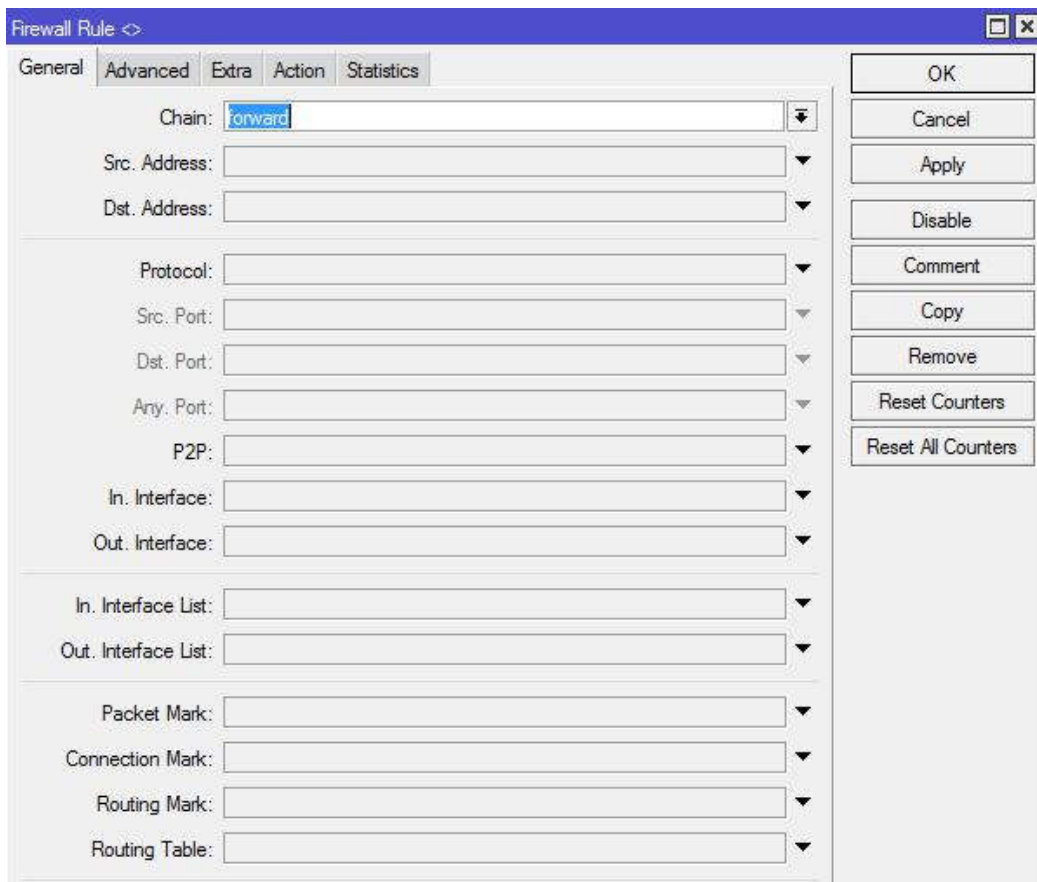
Setelah mempelajari Mikrotik sekitar 1 bulan ia belajar dan mengumpulkan uang, ia mendapat ide yang sangat cemerlang, ia memiliki inisiatif ingin membuat hotspot di rumahnya karena ia melihat sinyal HP di desanya sangatlah susah. Akhirnya ia membuat hotspot dan membeli internet dari ISP, akhirnya hotspot Jono-pun berhasil menyebar ke seluruh penjuru desa, penduduk desapun mulai banyak yang memakai. Selang beberapa minggu kalangan ibu-ibu desa mulai resah karena anak-anak mereka mulai mengenal internet yang luas, gosip-gosip ibu-ibu tersebutpun sampai ke telinga Jono. Jono mulai memikirkan bagaimana caranya agar anak-anak atau remaja- remaja desa tidak membuka yang aneh-aneh. Sampai akhirnya Jono menemukan materi atau pembahasan Blok Konten, menurut ia pembahasan itu sangatlah cocok dengan permasalahannya, Jono akan memblokir situs yang berbau porno, perjudian, dan lain-lain yang kira-kira berbau negative. Akhirnya setelah berunding dengan kru-nya ia menerapkan fitur blok konten tersebut. Yap permasalahan pun kellar dan berjalan lancar, ia pun sekarang sudah tidak kekurangan uang saku lagi, selain belajar ia juga dapat menghasilkan fulus. Mantab bukan ? "menyelam sambil minum air."

Oke langsung ke materi aja ya, dalam praktek ini kita akan memblokir beberapa konten besar yang biasanya sulit diblok menggunakan IP. Yaitu Facebook, Twitter, dan Porno. Langsung ke stepnya ya sob :

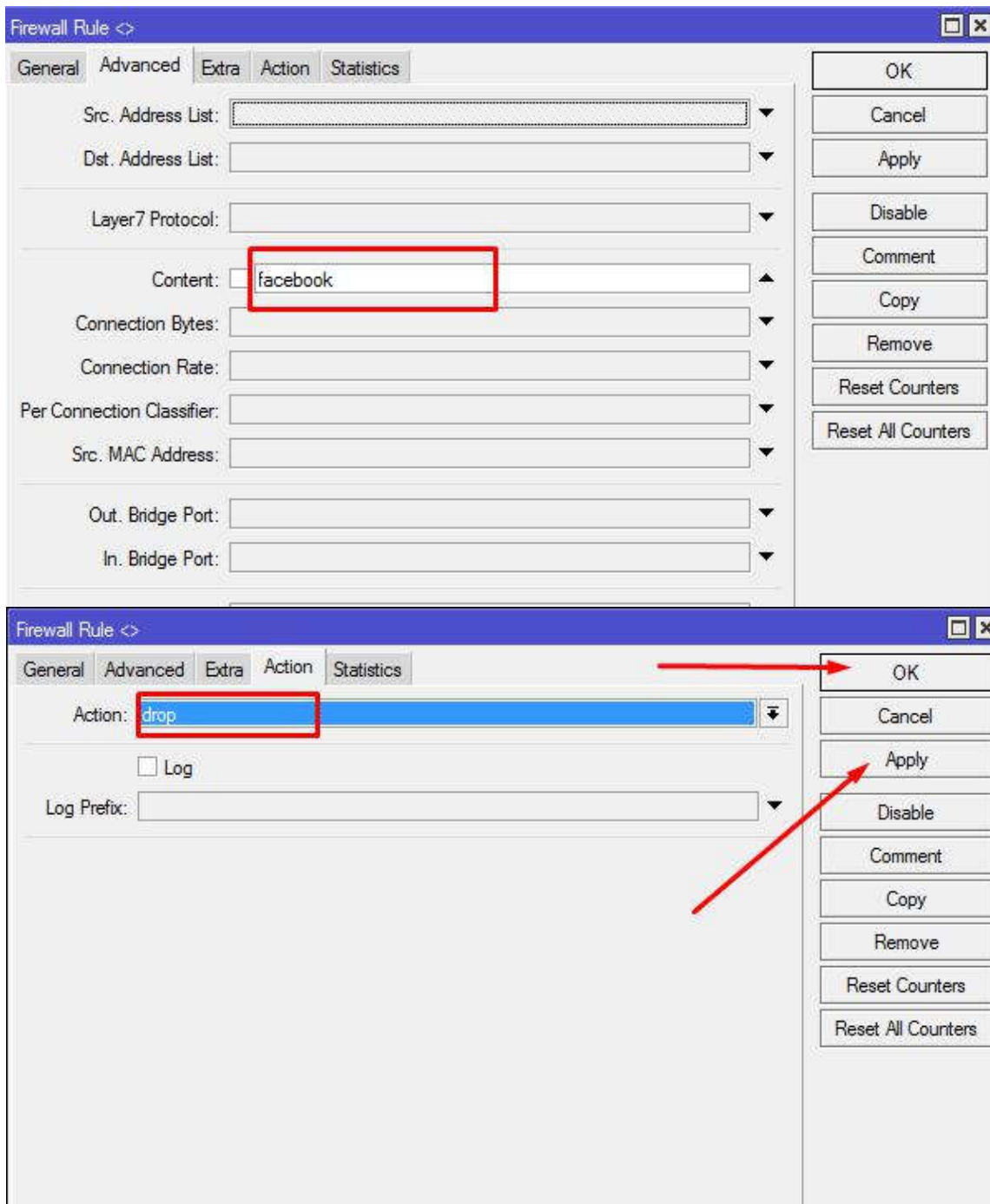
1. Siapkan perangkat Mikrotik anda dan PC anda. Colok-colokin dulu.
2. Koneksikan PC anda ke internet melalui perangkat Mikrotik anda.
3. Masuklah ke Menu **IP>Firewall>Filter Rule>add**.



4. Kemudian di **General**, isi **Chain=forward**, lalu Tab ke **Advanced** dan isi di **Content=facebook**, lalu di **Action** isi dengan **Action=drop**, lalu



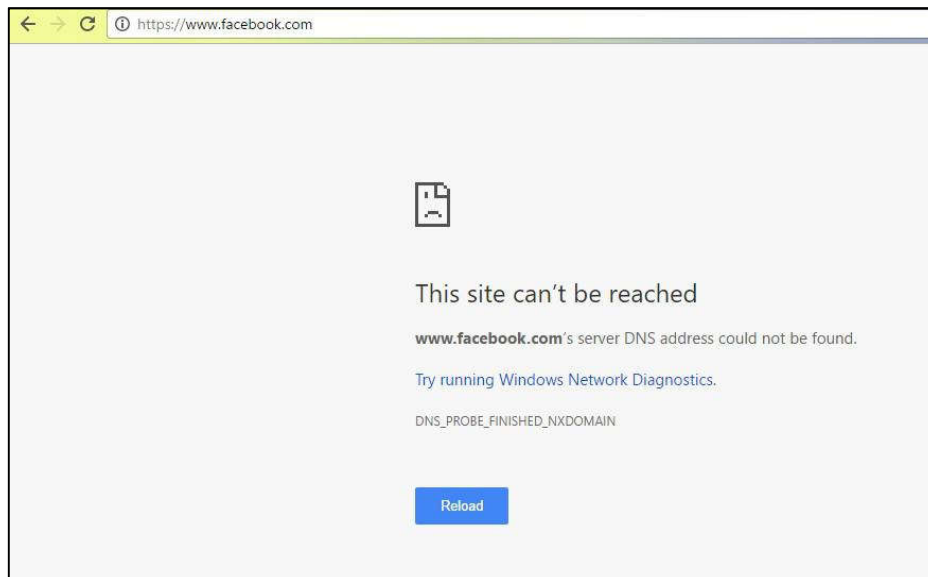
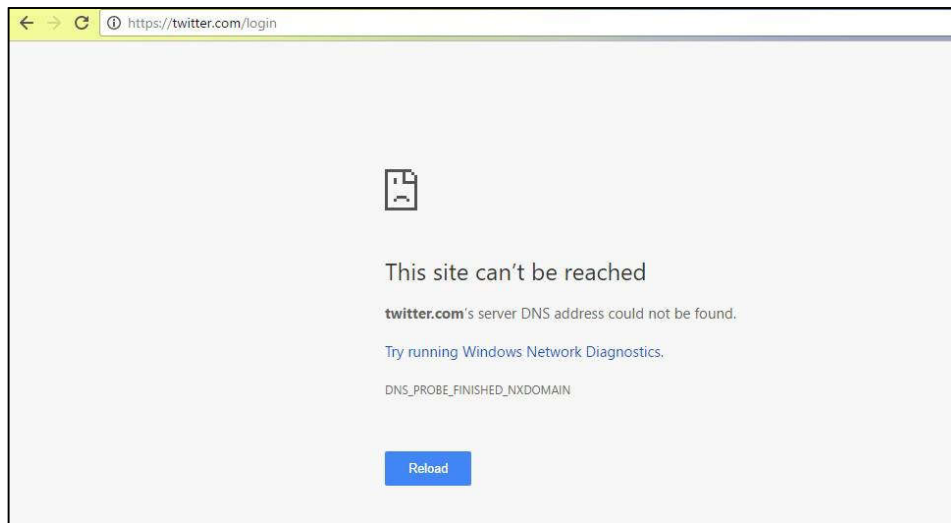
**Apply dan OK.**



5. Ulangi step ke 4 dengan Content= Twitter dan juga Porn, sehingga di filter rules terdapat 3 content yang di drop atau ditolak.

Firewall										
Filter Rules										
NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols										
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📁</div> <div>🔍</div> <div>00 Reset Counters</div> <div>00 Reset All Counters</div> <div>Find</div> <div>all</div> <div>▼</div> </div>										
#	Action /	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Byte
1	✗ drop	forward								
2	✗ drop	forward								
0	✗ drop	forward								16.8

6. Cobalah Client untuk membuka 3 konten tadi, apakah masih bisa atau sudah keblok ?

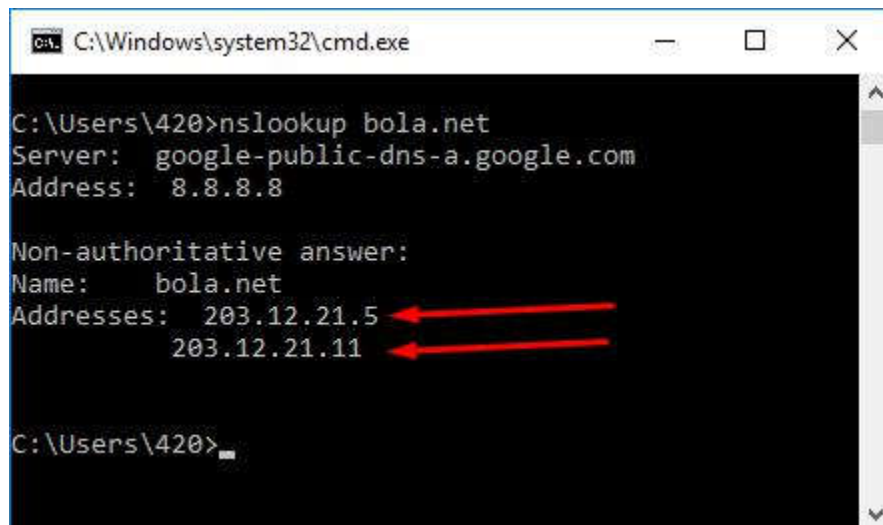


KeBlok bukan? Apabila ada orang atau client yang ingin mengakses lewat perangkat Mikrotik yang sudah dikonfigurasi seperti tadi (blok konten), mereka tidak bisa membuka situs-situs yang mengandung unsur facebook, twitter, dan porn. Aman bukan? maka dari itu, selamatkan generasi bangsa kita ya guys.

## LAB 16 Blok Situs Dengan Address list

Jika pada lab sebelumnya kita mencoba mem-Blokir situs menggunakan Content, di lab ini kita akan mencoba mem-Blokir situs menggunakan Address List, Apa Fungsi dari Address List? Address list berfungsi untuk mengelompokkan Banyak IP/Domain ke dalam satu Kelompok, address list akan di gunakan untuk mem-Blokir suatu situs ketika situs tersebut menggunakan banyak IP address (Lebih dari satu), jika kita mem-Blokir suatu website yang menggunakan banyak IP Address dengan Filter Rule maka kita akan membuat banyak Rule dan itu Ribet... berbeda jika kita mem-Blokir suatu website yang menggunakan banyak IP Address dengan Address List, Kita hanya perlu membuat satu address list dan 1 Rule Firewall... di lab ini kita akan mencoba memblokir website bola.net..

Pertama kita lihat ip address yang di gunakan Website bola.net



```
C:\Windows\system32\cmd.exe

C:\Users\420>nslookup bola.net
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:     bola.net
Addresses: 203.12.21.5
           203.12.21.11

C:\Users\420>
```

Website bola.net memakai 2 IP Address.. Setelah kita mengetahui IP Address yang di gunakan oleh website bola.net kita perlu membuat address list untuk website tersebut..

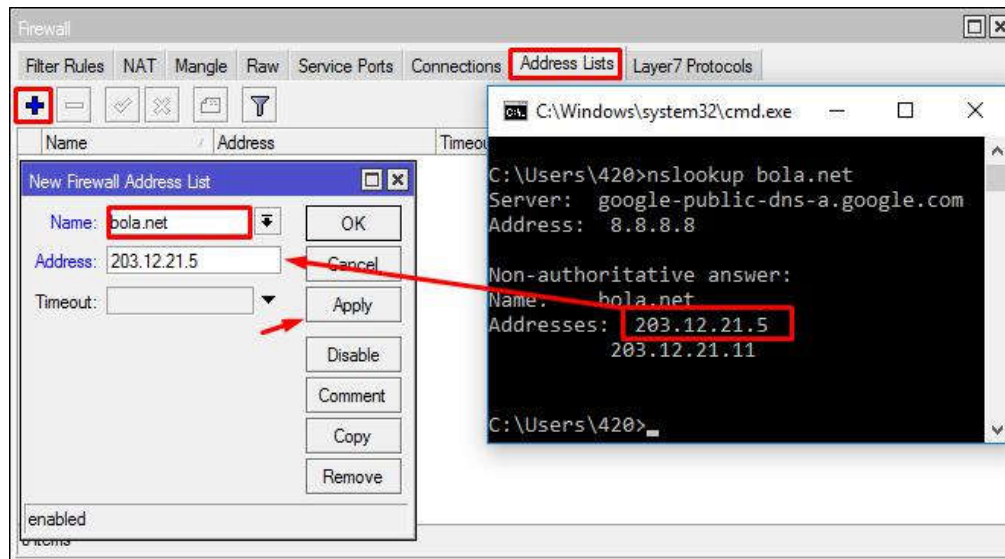
Klik IP > Firewall > Address List > Add(+)

Isi Nama=Bola.net (Bebas)

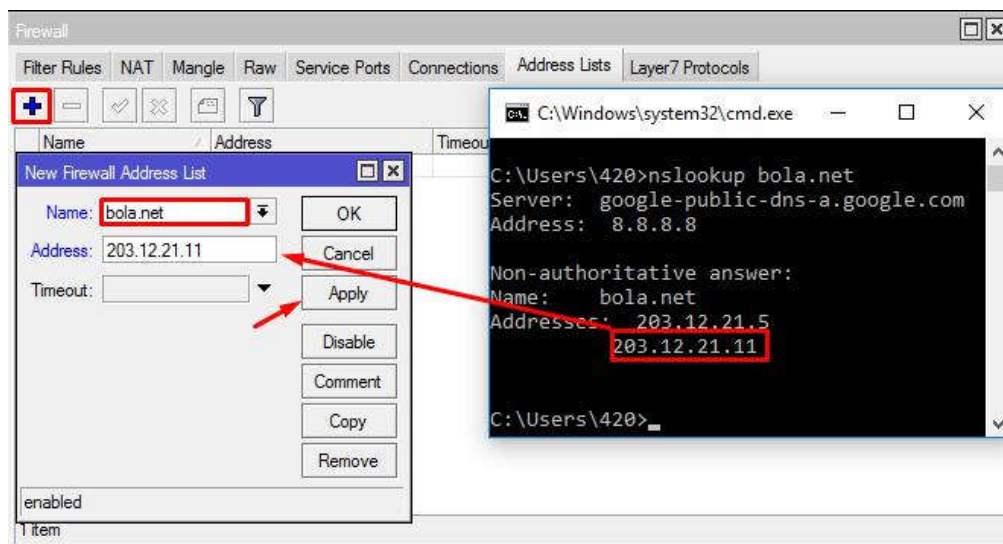
Masukan salah satu IP yang di gunakan Website Bola.net

Lalu Apply dan OK



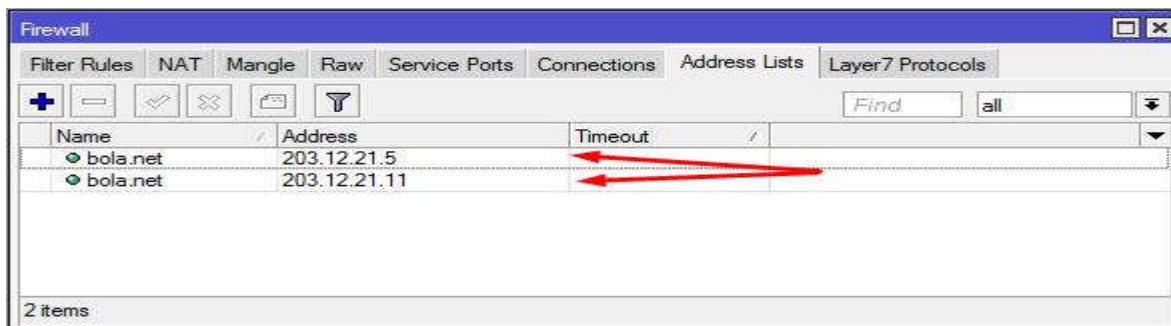


Ulangi cara di atas dan masukan IP address kedua yang di gunakan Bola.net



Step selanjutnya adalah membuat Filter rule dan memasukan Address list ke Filter rule tersebut...

Address List Bola.net

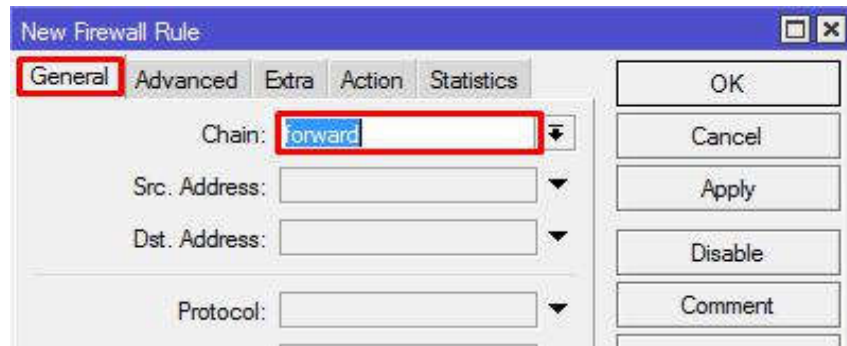


Masuk Ke Menu Filter Rule terlebih dahulu..

- Klik IP > Firewall > Filter Rule > Add (+)



- Klik General dan isi Chain=Forward



Selanjutnya isi kita masukan Address list ke Filter Rule...

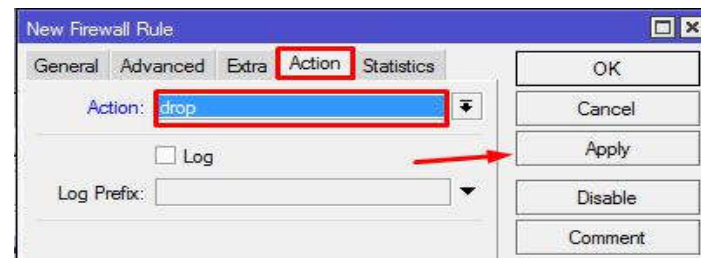
Klik Advance > Isi Dst.Address List=Bola.net

Selanjutnya adalah memilih action=Drop untuk filter rule tersebut

Klik Action > Isi Action=Drop



Lalu Apply dan OK



Setelah step ini maka Website Bola.net sudah terblokir...

Untuk Src.Address/Client yang ingin di blokir bisa di isi dengan IP Network,IP Range

/Kita bisa menggunakan Fitur Not (!), Isi Src.Address sesuai Kebutuhan kita...

Address list juga bisa kita gunakan untuk memblokir beberapa Website sekaligus..

Contoh saya akan mencoba memblokir beberapa situs belanja Online seperti = OLX.com Mataharimall.com ,Tokopedia.com...

Peratama kita cari IP address yang di gunakan oleh ketiga website tesebut...

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\420>nslookup mataharimall.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: mataharimall.com
Address: 139.255.59.18

C:\Users\420>nslookup olx.co.id
Server: google-public-dns-a.google.com
Address: 8.8.8.8

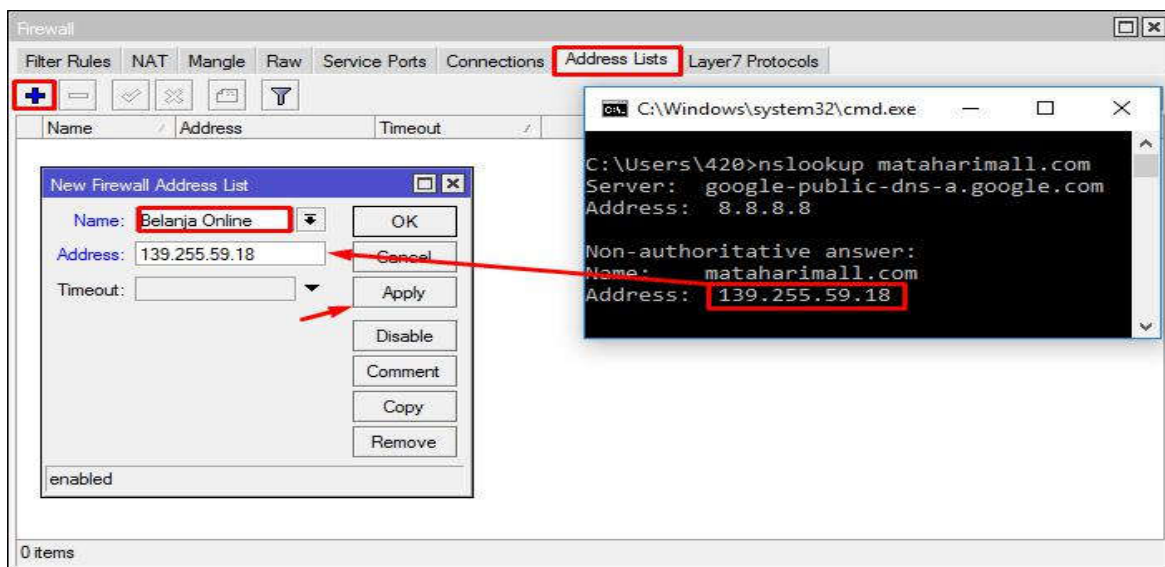
Non-authoritative answer:
Name: olx.co.id
Addresses: 210.210.179.84
           210.210.179.94
           210.210.179.104

C:\Users\420>nslookup tokopedia.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: tokopedia.com
Addresses: 182.253.224.184
           182.253.224.188
```

Website Mataharimall menggunakan 1 IP address, OLX.co.id menggunakan 3 IP Address ,dan Tokopedia.com menggunakan 2 IP Address....

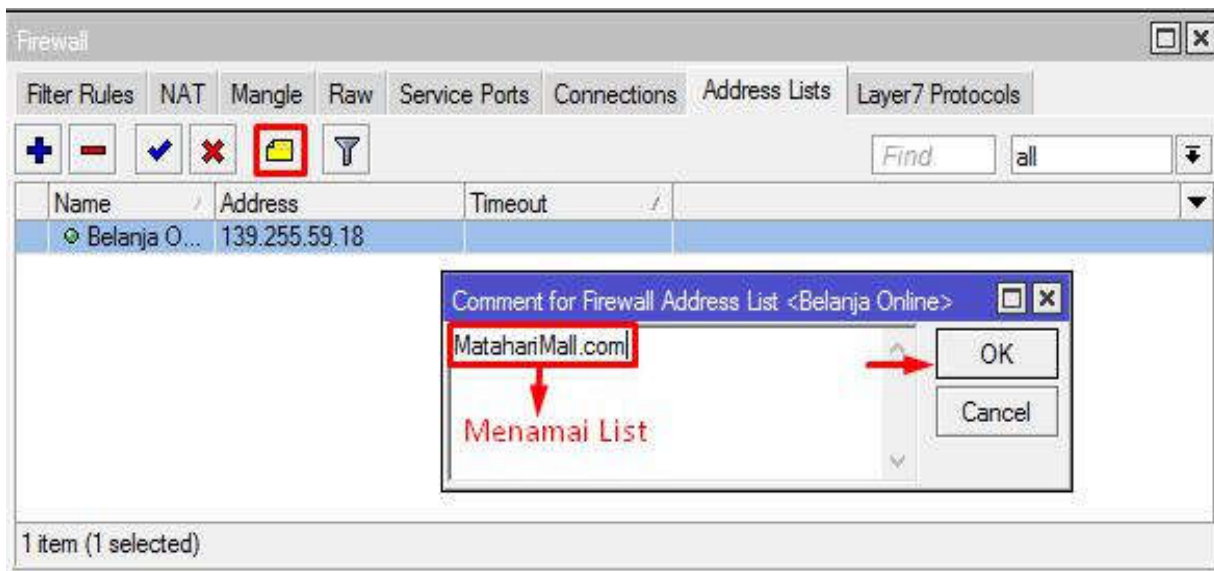
Selanjutnya kita hanya perlu mengelompokkan ke-Enam IP tersebut ke dalam 1 Address List yang di beri nama Belanja Online....



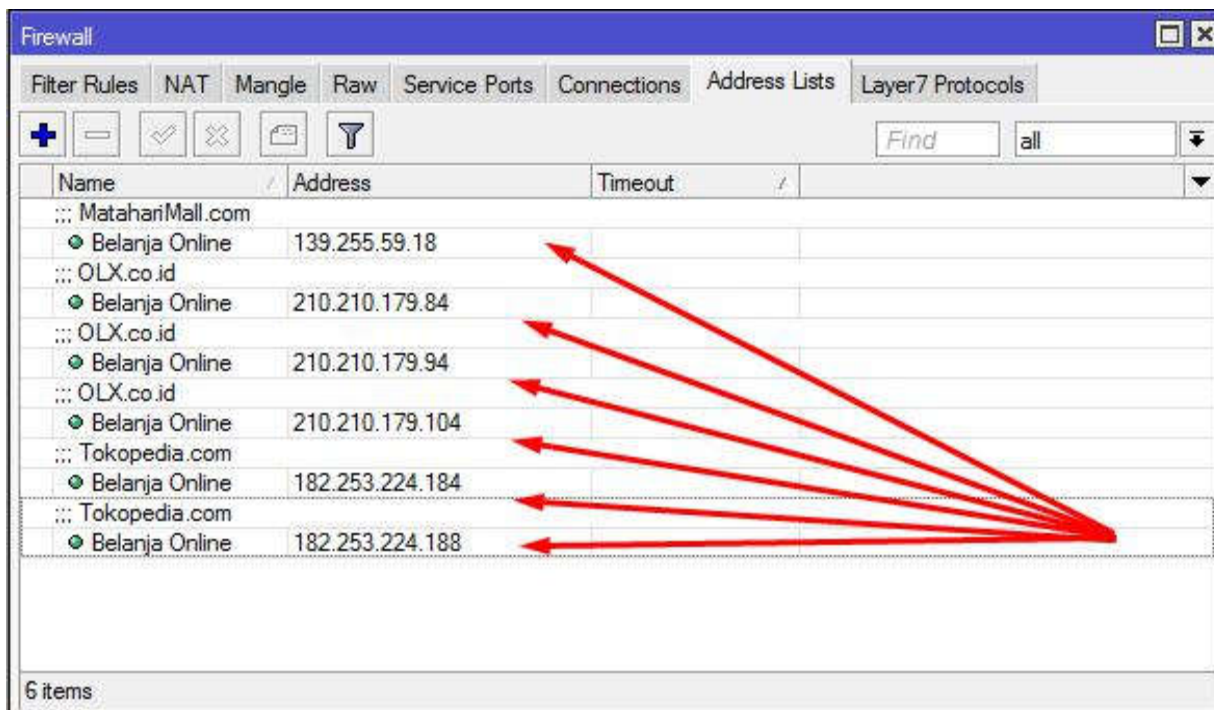
Lakukan Berulang kali dan Masukan IP Address yang di gunakan OLX.co.id dan Tokopedia.com ke dalam Address List=Belanja Online...

Jika sudah Memasukan Semua IP Address ke Address List=Belanja Online kita perlu Memberi Comment di List yang telah kita buat yang berfungsi untuk

menamai/menandai mana IP Address Mataharimall dan yang mana IP Address OLX.co.id,



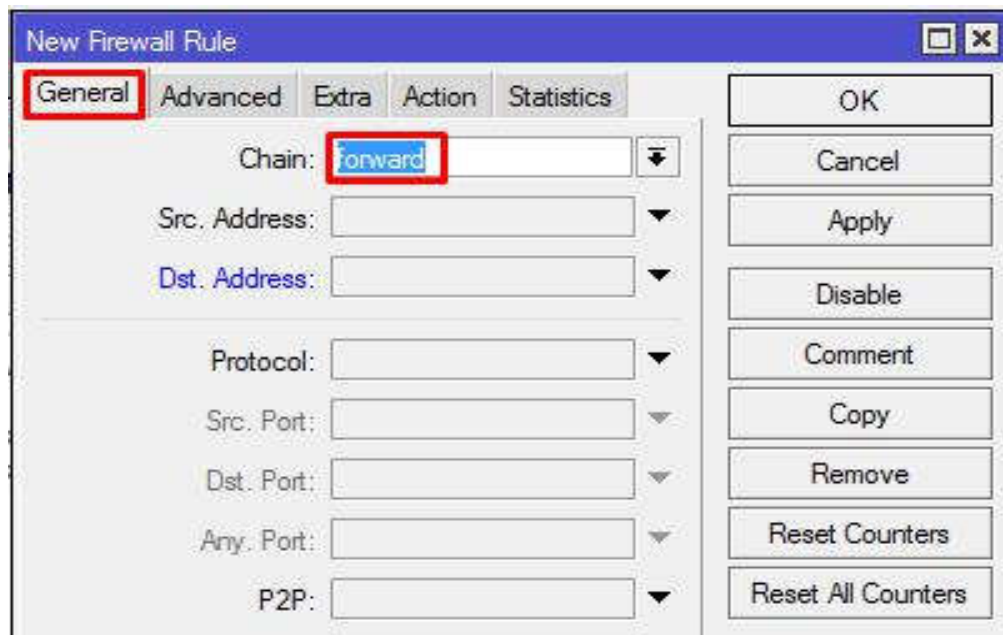
Jika kita memberi Comment di setiap List maka Hasil nya akan Seperti Ini



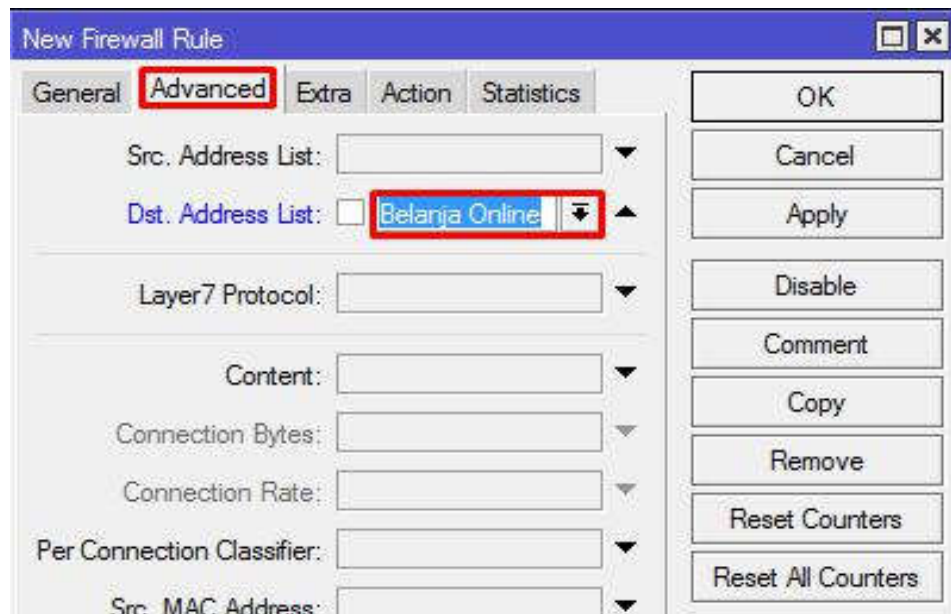
Jika sudah membuat address list,selanjutnya kita akan membuat Filer Rule dan memasukan Address list ke Filter Rule...

Filter Rule > Add (+)

Isi Chain=Forward

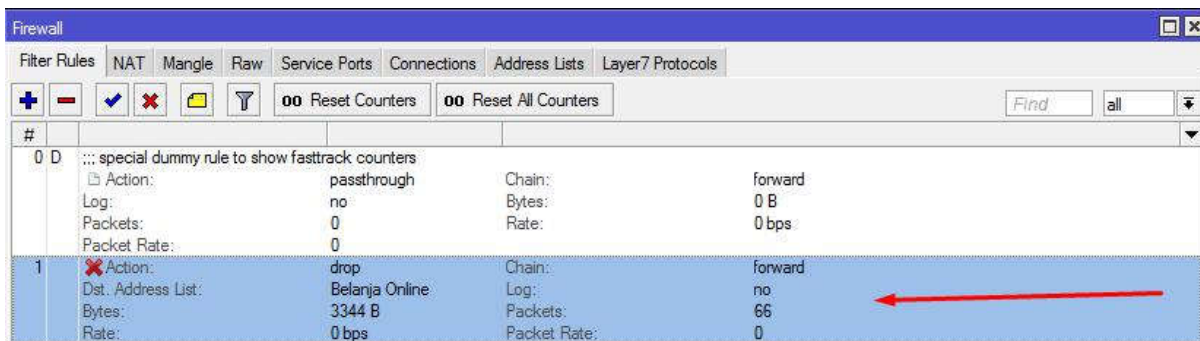
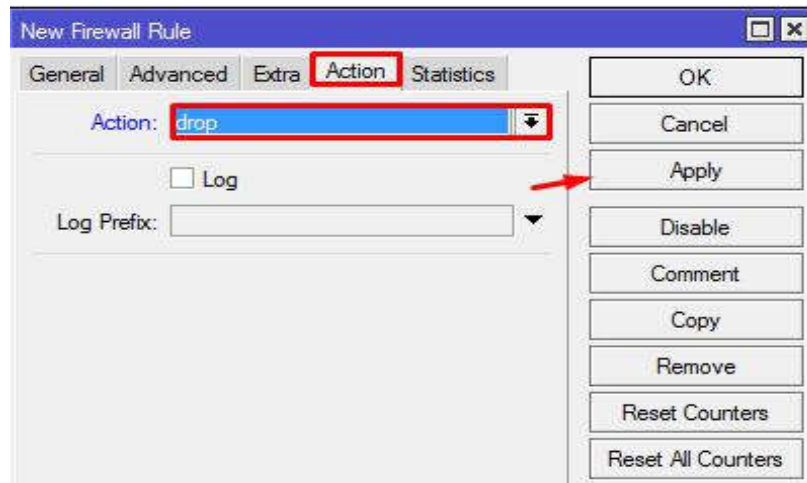


Dan Isi Dst.Address List=Belanja Online



Dan isi Action=Drop

Lalu Apply dan OK



Coba test masuk ke 3 Webiste tersebut.. maka hasil nya akan Eror



## LAB 17 Block Remote Access

Pada lab kali ini saya akan membuat sebuah lab yang berguna untuk melindungi router kita juga dari tangan - tangan jahil yang sering mengganggu sebuah jaringan, dalam lab pertama dalam firewall kita melindungi router dengan menggunakan IP untuk keamanannya, namun dalam lab kali ini kita akan melindungi router dari hacker yang mencoba me remote access melalui telnet/ssh/ webfig, DLL.

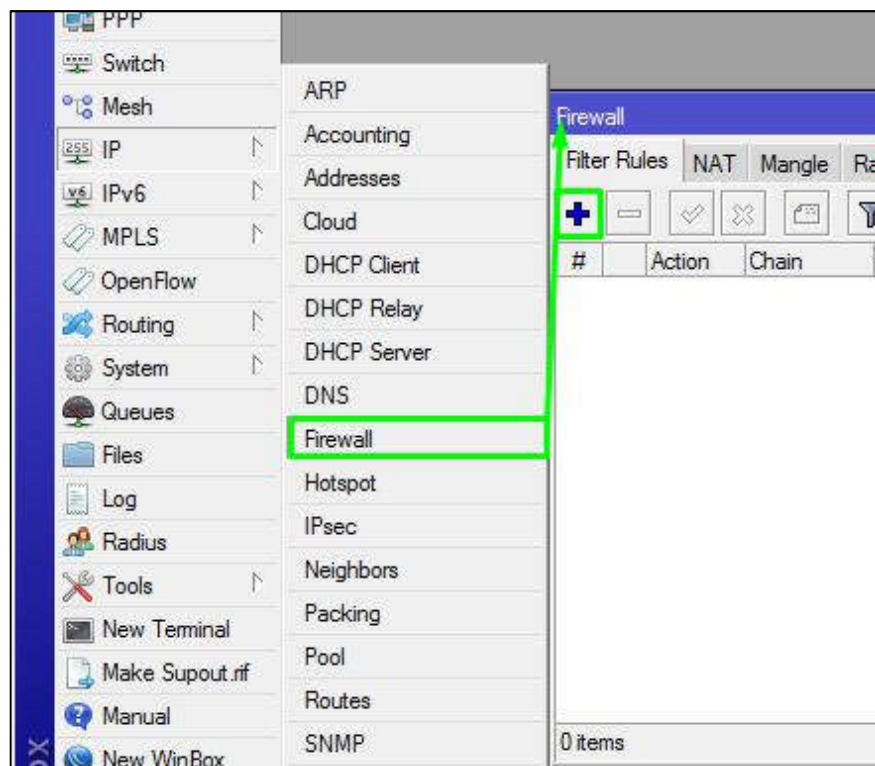
Dalam lab kali ini kita akan mencoba memblok **ssh**(port TCP 22), **telnet**(port TCP 23), **ping**(UDP), **webfig**(TCP 80). Berikut langkah - langkah untuk memblok remote access :

Catatan : daftar port dalam dunia jaringan bisa diakses :

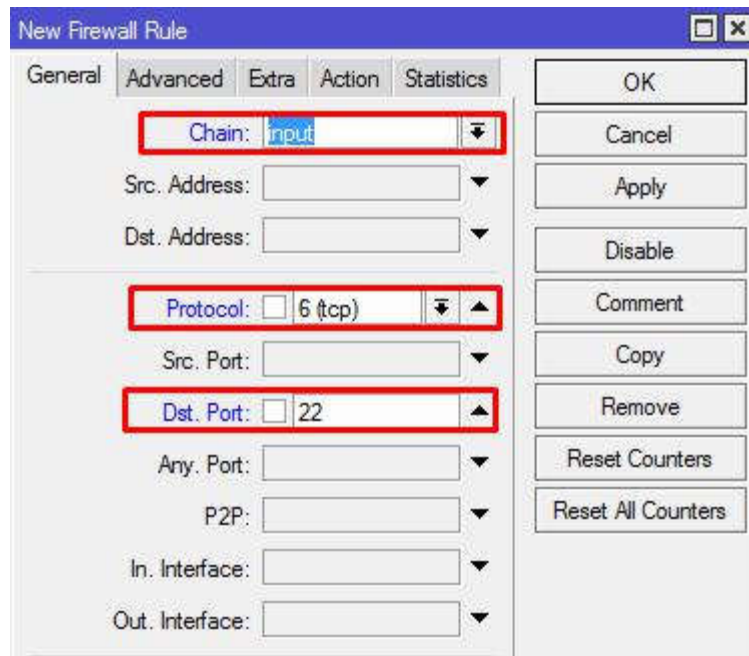
[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

### A. Blok SSH

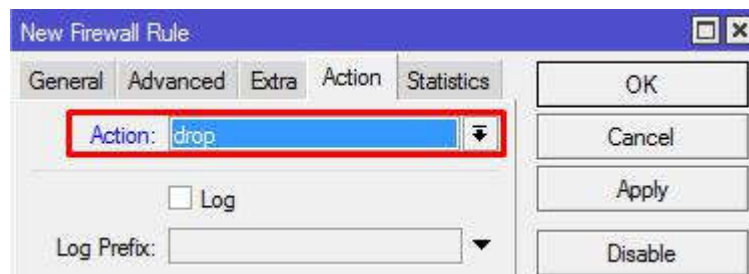
1. Pertama, masuk ke winbox dan klik menu **IP> firewall> filter rule> add.**



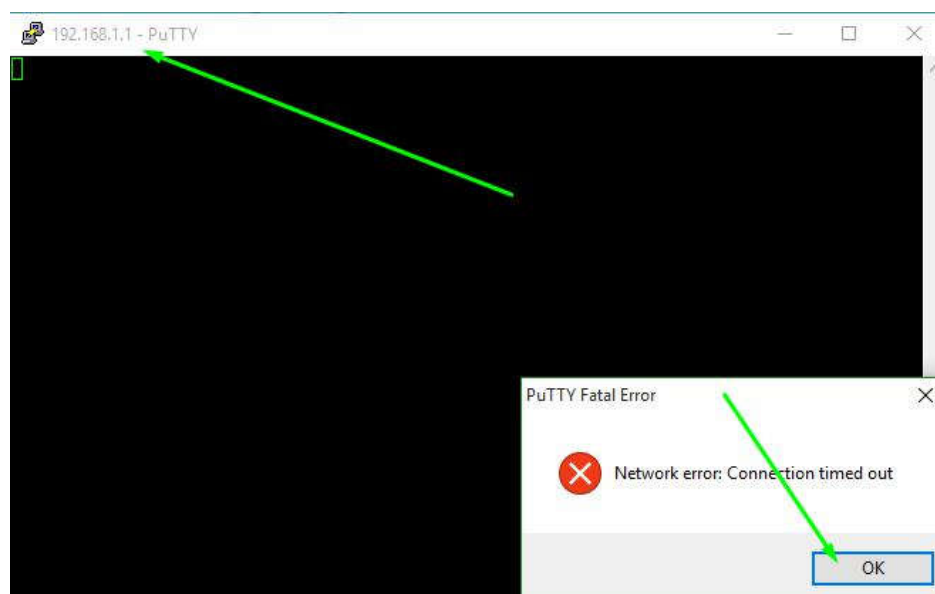
2. Masukan disana **chain=input**,  
**protocol=TCP**, **dst.port=22**(port SSH)



3. Jika sudah pindah ke tab **Action** > **Action=drop**. Apply, OK.



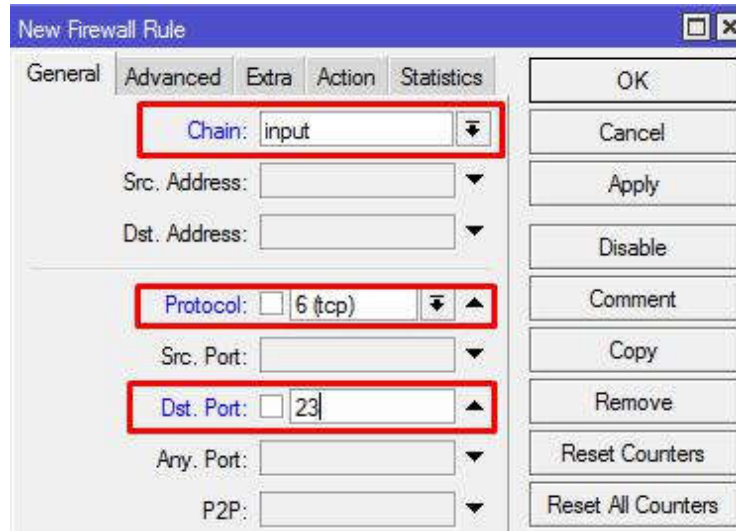
4. Jika sudah di setting, cobalah untuk meremote access IP router menggunakan SSH (memakai PUTTY).



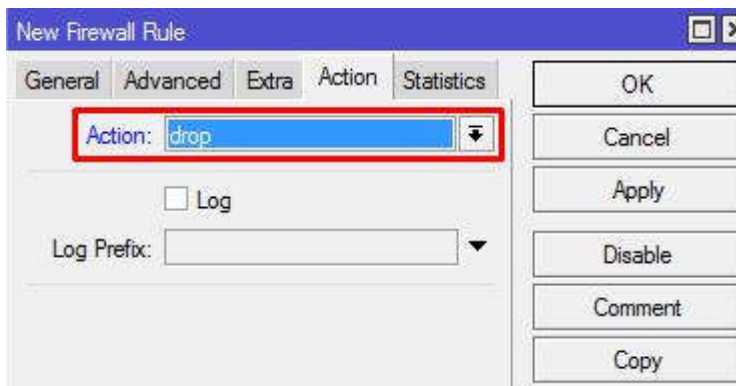
Jika muncul seperti diatas, berarti anda telah gagal untuk mengSSH router anda, dan jika anda gagal berarti anda berhasil memblok SSH tersebut..

#### A. Blok Telnet

1. Masuk menu **IP> firewall> filter rule> add**.
2. Masukkan **chain=input**, **protocol=TCP**, **dst.port=23** (port Telnet).



3. Masuk ke tab **Action>action=drop**, apply, OK.



4. Terakhir, untuk mengecek blok kita berhasil/  
tidak cobalah untuk mentelnet(melalui CMD) IP  
router kita sendiri. Maka akan seperti ini.

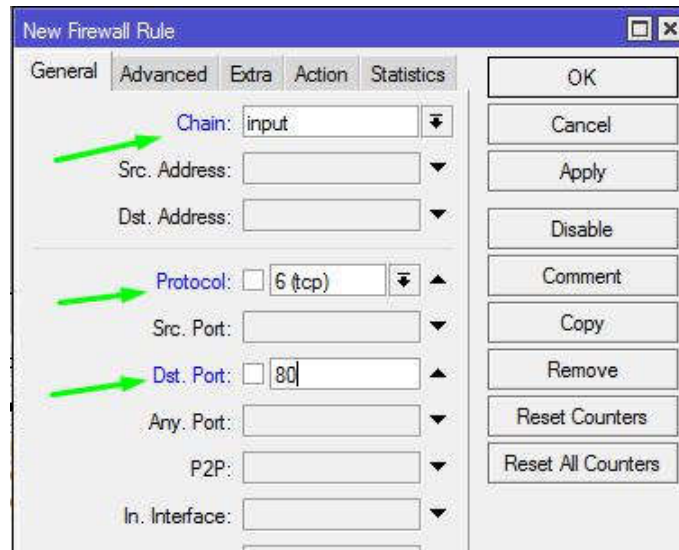
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Lenovo>telnet 192.168.11.1
Connecting To 192.168.11.1...Could not open connection to the host, on port 23: Connect failed
```

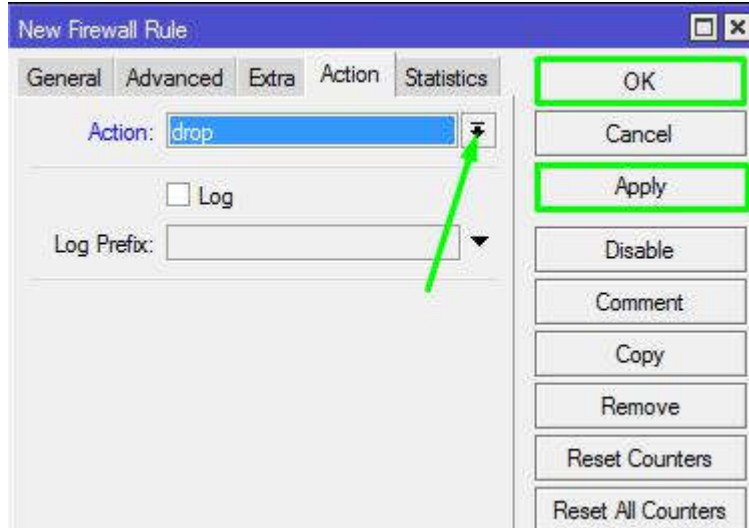


## B. Blok webfig

1. Masuk menu **IP > firewall > filter rule > add**.
2. Masukkan disana **chain=input**, **protocol=TCP**, **dst.port=80**(port webfig).

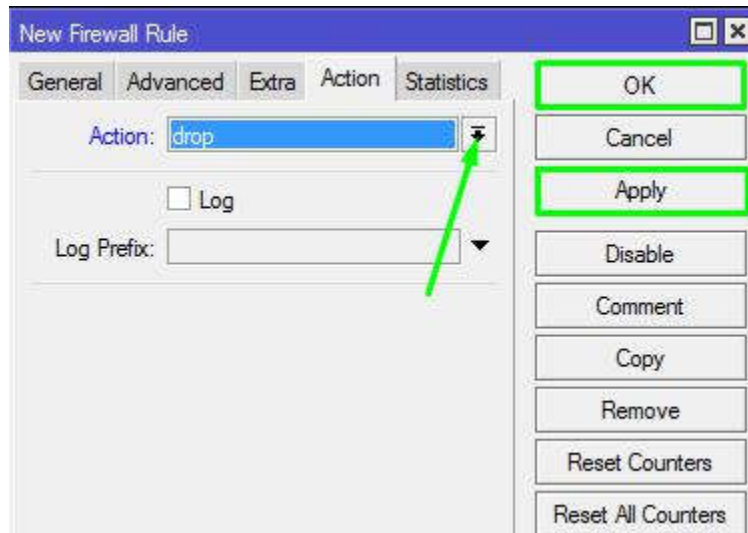


3. Masuk tab **Action > action=drop**, apply, OK.



4. Untuk percobaan pengetesan coba login melalui webfig IP router kita.





4. Terakhir untuk telnet ini coba ping ke router kita.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\HP>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Pasti akan Request Time Out, karena sudah kita blok yang mencoba remote access ping tersebut...

Block akses cara ini bisa anda atur sesuai dengan kebutuhan, misalkan pada kali ini tujuan kita memblokir Telnet, SSH, dan Webfig adalah demi masalah keamanan, jadi anda membuat aturan yang mengharuskan hanya menggunakan Winbox jika ingin mengkonfigurasi, tidak bisa dengan Telnet, SSH, dan Webfig.

## LAB 18 Block Situs Dengan Layer 7 Protocol

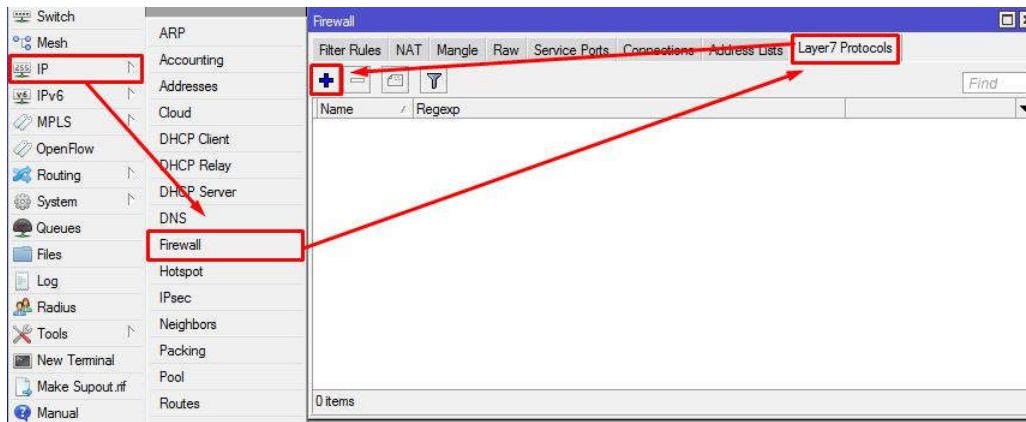
Pada Lab kali ini kita akan mencoba memblokir suatu situs, misalnya facebook dengan menggunakan Mikrotik Layer 7 Protokol (L7). Protokol Layer7 adalah metode untuk mencari pola dalam ICMP/TCP/UDP stream, atau istilah lainnya regexp pattern.

Cara kerja L7 adalah mencocokkan (matcher) 10 paket koneksi pertama atau 2KB koneksi pertama dan mencari pola/pattern data yang sesuai dengan yang tersedia. Jika pola ini tidak ditemukan dalam data yang tersedia, matcher tidak memeriksa lebih lanjut. Dan akan dianggap unknown connections. Anda harus mempertimbangkan bahwa banyak koneksi secara signifikan akan meningkatkan penggunaan memori pada RB maupun PC Router anda. Untuk menghindari hal tersebut, maka tambahkan regular firewall matchers (pattern) untuk mengurangi jumlah data yang dikirimkan ke layer-7 filter.

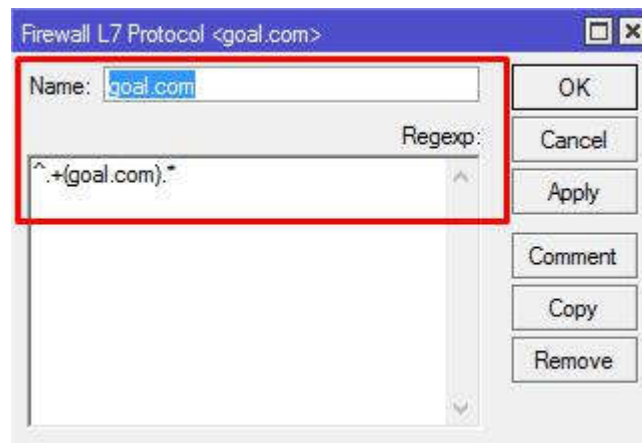
Layer 7 matcher harus melihat kedua arah lalu lintas (masuk dan keluar). Untuk memenuhi persyaratan ini rule L7 harus diatur dalam chain Forward. Jika rule pada chain input/prerouting, maka aturan yang sama juga harus diatur dalam chain output/postrouting, jika tidak, maka data mungkin dianggap tidak lengkap sehingga pola/pattern dianggap tidak benar/cocok.

Oke, langsung saja kita coba bagaimana caranya.

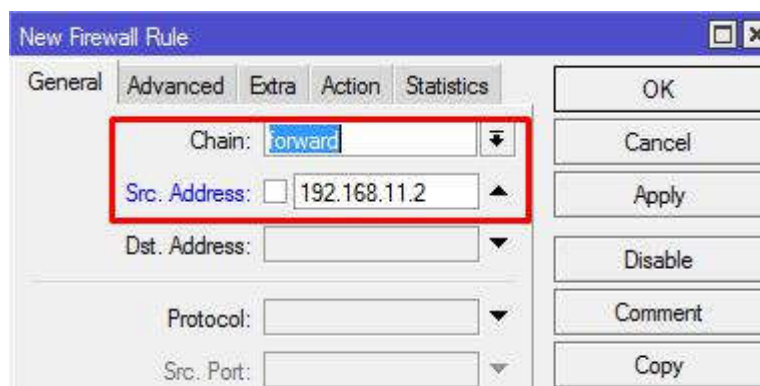
1. Buka Winbox terlebih dahulu dan pastikan anda terkoneksi dengan internet hanya menggunakan RouterBoard.
2. Masuk pada menu **IP** kemudian **Firewall** lalu pilih tab **Layer 7 Protocol** kemudian **Add**.



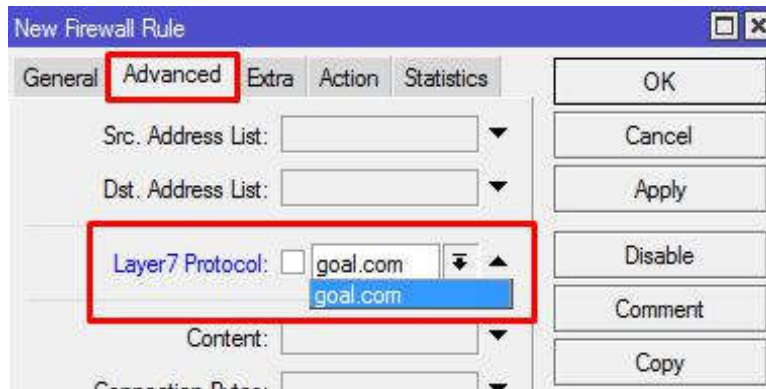
3. Pada kali ini kita akan mencoba untuk memblokir situs [www.goal.com](http://www.goal.com), Selanjutnya masukan name=goal.com, Ragexp: `^.(goal.com).*` (ingat penulisan tandanya harus sama persis) apply, OK. Jika perintah tersebut masih gagal/ tidak berhasil masukan perintah Ragexp: `^.(goal.com).*$`



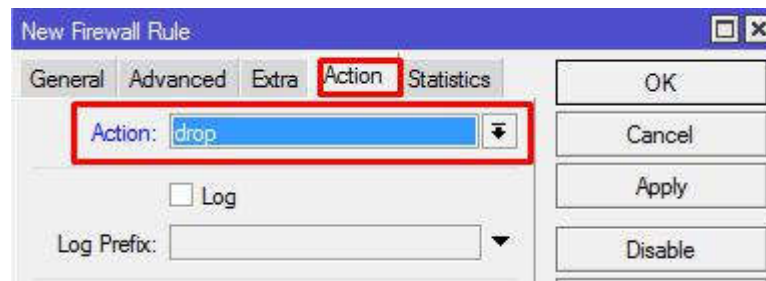
Jika sudah membuat Layer 7 Protocolnya, selanjutnya masuk menu **Filter Rule > Add**. **Chain=forward** kemudian isikan **Src.address=192.168.11.2**. IP dari Src.Address tersebut adalah IP PC yang tidak diperbolehkan untuk mengakses situs yang telah di blokir tadi, untuk percobaan gunakan saja IP PC anda agar anda sendiri dapat membuktikan nanti apakah konfigurasinya berhasil atau gagal.



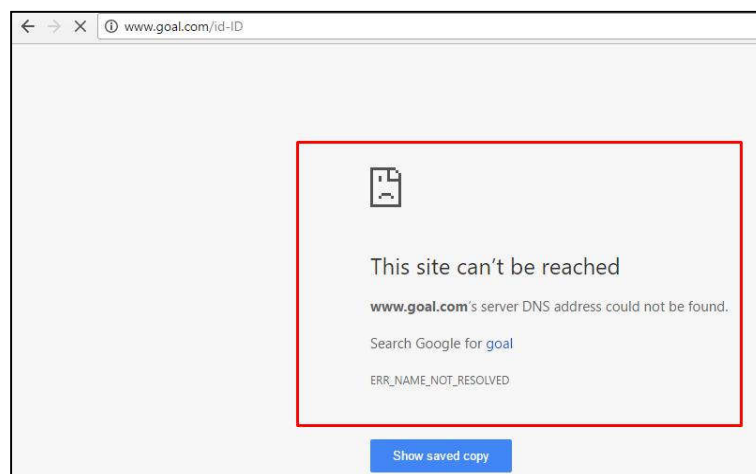
4. Kemudian masuk ke Tab **Advanced**, isikan kolom **Layer7Protocol** dengan **goal.com** tadi.



5. Kemudian masuk ke Tab **Action** dan isikan kolom **Action=drop**.



6. Coba sekarang anda tes akses situs [www.goal.com](http://www.goal.com) dari PC anda tersebut / dari PC yang IP nya dilarang untuk mengakses situs tersebut. Bisa terbuka atau tidak, jika tidak berarti anda berhasil. Dan pastikan juga PC anda tidak terkoneksi menggunakan Wireless anda sendiri, tetapi terkoneksi hanya menggunakan Router.



Sukses sudah, PC yang anda tetapkan tadi tidak akan bisa membuka situs [www.goal.com](http://www.goal.com) tersebut.



## LAB 19 Connection Tracking

Dalam firewall, ada yang di sebut dengan Connection Tracking yang merupakan fitur baru di dalam firewall yang ditambahkan saejak kernel 2.4.x. Kemampuan dari connection tracking adalah untuk menyimpan dan menjaga informasi koneksi seperti koneksi baru atau koneksi yang sudah ada yang disertai dengan jenis protokol, alamat IP asal dan alamat IP tujuan. Dengan menggunakan fitur ini, para administrator dapat menolak atau mengijinkan berbagai macam koneksi.

Connection tracking mempunyai beberapa keadaan: Dalam mikrotik, bisa dilihat di Menu: Ip > Firewall > Connections

Firewall									
Filter Rules NAT Mangle Raw Service Ports <b>Connections</b> Address Lists Layer7 Protocols									
Tracking									
	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes	
C	0.0.0.0:5678	255.255.255.255:5678	17 (u...		00:00:03		0 bps/0 bps	465 B/0 B	
C	192.168.1.1:41386	255.255.255.255:5678	17 (u...		00:00:01		0 bps/0 bps	152 B/0 B	
C	192.168.10.1:51424	255.255.255.255:5678	17 (u...		00:00:03		0 bps/0 bps	450 B/0 B	
SCs	192.168.10.254	8.8.8.8	1 (c...		00:00:09		960 bps/960 bps	18.8 KiB/18.5 KiB	
C	192.168.10.254:5678	255.255.255.255:5678	17 (u...		00:00:01		0 bps/0 bps	96 B/0 B	
SACs	192.168.10.254:49154	216.58.203.242:443	6 (tcp)		23:59:57	established	0 bps/0 bps	3864 B/6.1 KiB	
SACs	192.168.10.254:49155	74.125.68.181:443	6 (tcp)		23:59:21	established	0 bps/0 bps	2652 B/5.3 KiB	
SACs	192.168.10.254:49164	172.217.24.110:443	6 (tcp)		23:59:52	established	0 bps/0 bps	31.3 KiB/584.9 KiB	
SACs	192.168.10.254:49178	54.194.99.187:443	6 (tcp)		23:59:34	established	0 bps/0 bps	82 B/80 B	
SACs	192.168.10.254:49179	54.194.99.187:443	6 (tcp)		23:59:24	established	0 bps/0 bps	82 B/80 B	
SACs	192.168.10.254:49180	202.154.59.183:80	6 (tcp)		23:59:29	established	0 bps/0 bps	3835 B/44.5 KiB	
SACs	192.168.10.254:49181	202.154.59.183:80	6 (tcp)		23:59:28	established	0 bps/0 bps	6.1 KiB/68.4 KiB	
SACs	192.168.10.254:49185	202.154.59.183:80	6 (tcp)		23:59:28	established	0 bps/0 bps	4157 B/15.3 KiB	
SACs	192.168.10.254:49186	202.154.59.183:80	6 (tcp)		23:59:28	established	0 bps/0 bps	8.6 KiB/184.2 KiB	
SACs	192.168.10.254:49187	202.154.59.183:80	6 (tcp)		23:59:28	established	0 bps/0 bps	4309 B/32.9 KiB	
SACs	192.168.10.254:49188	52.9.56.132:443	6 (tcp)		23:59:26	established	0 bps/0 bps	82 B/40 B	
SACs	192.168.10.254:49194	74.125.68.94:443	6 (tcp)		23:59:52	established	0 bps/0 bps	1345 B/792 B	
SACs	192.168.10.254:49197	74.125.200.148:443	6 (tcp)		23:59:52	established	0 bps/0 bps	3422 B/5.5 KiB	
SACs	192.168.10.254:49199	216.58.203.238:443	6 (tcp)		23:59:53	established	0 bps/0 bps	3088 B/37.8 KiB	
SACs	192.168.10.254:49204	192.0.72.28:80	6 (tcp)		23:59:23	established	0 bps/0 bps	1751 B/1188 B	
SACs	192.168.10.254:49205	192.0.72.28:80	6 (tcp)		23:59:23	established	0 bps/0 bps	1032 B/675 B	
SACs	192.168.10.254:49206	192.0.72.28:443	6 (tcp)		23:59:26	established	0 bps/0 bps	940 B/6.7 KiB	
SACs	192.168.10.254:49207	192.0.72.28:443	6 (tcp)		23:59:48	established	0 bps/0 bps	7.1 KiB/189.5 KiB	
SACs	192.168.10.254:49208	192.0.72.28:80	6 (tcp)		23:59:24	established	0 bps/0 bps	976 B/671 B	
SACs	192.168.10.254:49209	192.0.72.28:80	6 (tcp)		23:59:23	established	0 bps/0 bps	1711 B/638 B	
SACs	192.168.10.254:49210	192.0.72.28:80	6 (tcp)		23:59:23	established	0 bps/0 bps	990 B/605 B	
SACs	192.168.10.254:49211	202.154.59.183:80	6 (tcp)		23:59:52	established	0 bps/0 bps	5.5 KiB/65.4 KiB	
SACs	192.168.10.254:49212	192.0.72.28:443	6 (tcp)		23:59:24	established	0 bps/0 bps	903 B/507 B	
SACs	192.168.10.254:49213	192.0.72.28:443	6 (tcp)		23:59:26	established	0 bps/0 bps	1083 B/6.7 KiB	
SACs	192.168.10.254:49214	192.0.72.28:443	6 (tcp)		23:59:24	established	0 bps/0 bps	772 B/6.7 KiB	
SACs	192.168.10.254:49215	192.0.72.28:443	6 (tcp)		23:59:27	established	0 bps/0 bps	1098 B/564 B	
SAC	192.168.10.254:49218	192.168.10.1:8291	6 (tcp)		00:04:59	established	17.0 kbps/111.5 kbps	6.9 KiB/70.8 KiB	
SACs	192.168.10.254:53410	74.125.200.138:443	17 (u...		00:00:29		0 bps/0 bps	7.6 KiB/5.3 KiB	
SACs	192.168.10.254:53958	52.229.116.205:3544	17 (u...		00:02:31		0 bps/0 bps	1246 B/1644 B	
SACs	192.168.10.254:55130	172.217.24.110:443	17 (u...		00:00:05		0 bps/0 bps	7.8 KiB/16.3 KiB	

Connection tracking memiliki Fungsi untuk melihat semua informasi koneksi yang melewati router, seperti source dan destination IP dan Port yang sedang di gunakan, status koneksi,tipe protocol dan lain-lain. Setiap paket data itu memiliki status koneksi ( connection started ) yang dapat dilihat pada connection tracking, dan ini adalah Jenis-jenis status koneksi nya :

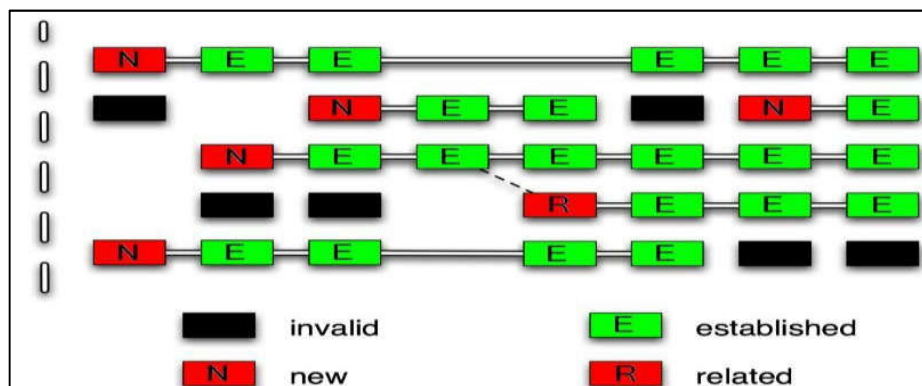
**Eestablished** = Sebuah koneksi yang merupakan bagian dari koneksi yang sudah ada. Maksudnya server 1 menerima paket SYN-ACK dan kemudian merespon dengan paket ACK (Acknowledgment). Intinya, paket tersebut adalah bagian dari koneksi yang telah dikenal.

**New** = Sebuah klien merequest koneksi melalui firewall. Maksudnya server1 menghubungi server2 dengan mengirimkan paket SYN (Synchronize), intinya, paket tersebut memulai koneksi baru atau memiliki koneksi yang belum melihat paket di kedua arah.

**related** = Sebuah koneksi yang mereques sebuah reques baru tetapi masih merupakan bagian dari koneksi yang sudah ada. Maksudnya server2 menerima paket SYN dari server 1 dan kemudian merespon dengan sebuah paket SYN-ACK (Synchronize-Acknowledgment), intinya, paket tersebut memulai koneksi baru, tetapi yang berhubungan dengan koneksi yang ada, seperti FTP transfer data atau pesan icmp yang error.

**invalid** = Sebuah keadaan dimana tidak ada keadaan seperti 3 keadaan di atas , intinya, paket tersebut tidak tergabung dalam connetion yang dikenal dan pada saat yang sama,paket teresbut tidak membuka koneksi baru yang valid.

Ini adalah gambaran connection state /status koneksi:





## LAB 20 Rule Connection State

Untuk apakah membuat rule untuk connection state...???

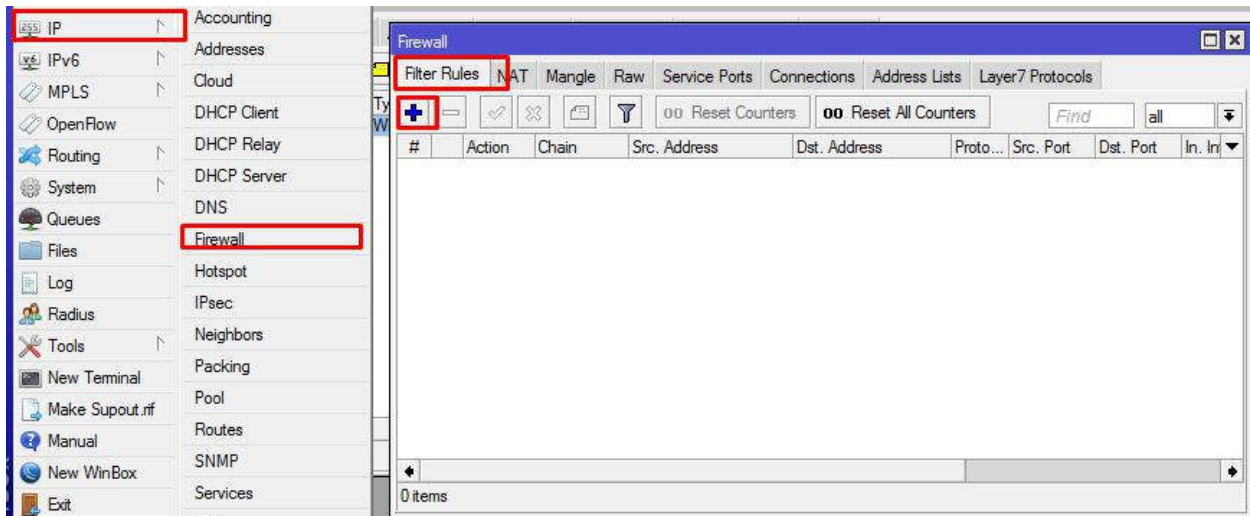
Fungsi dari membuat rule untuk connection state tidak lain adalah untuk menghemat system resource router kita, karna memang biasa nya setiap firewall di awali oleh degan filtering connection state, dan rule connection state di buat agar router kita pun juga lebih aman dan juga dapat lebih menhemat resource router kita.

Lalu bagaimanakah cara nya..??

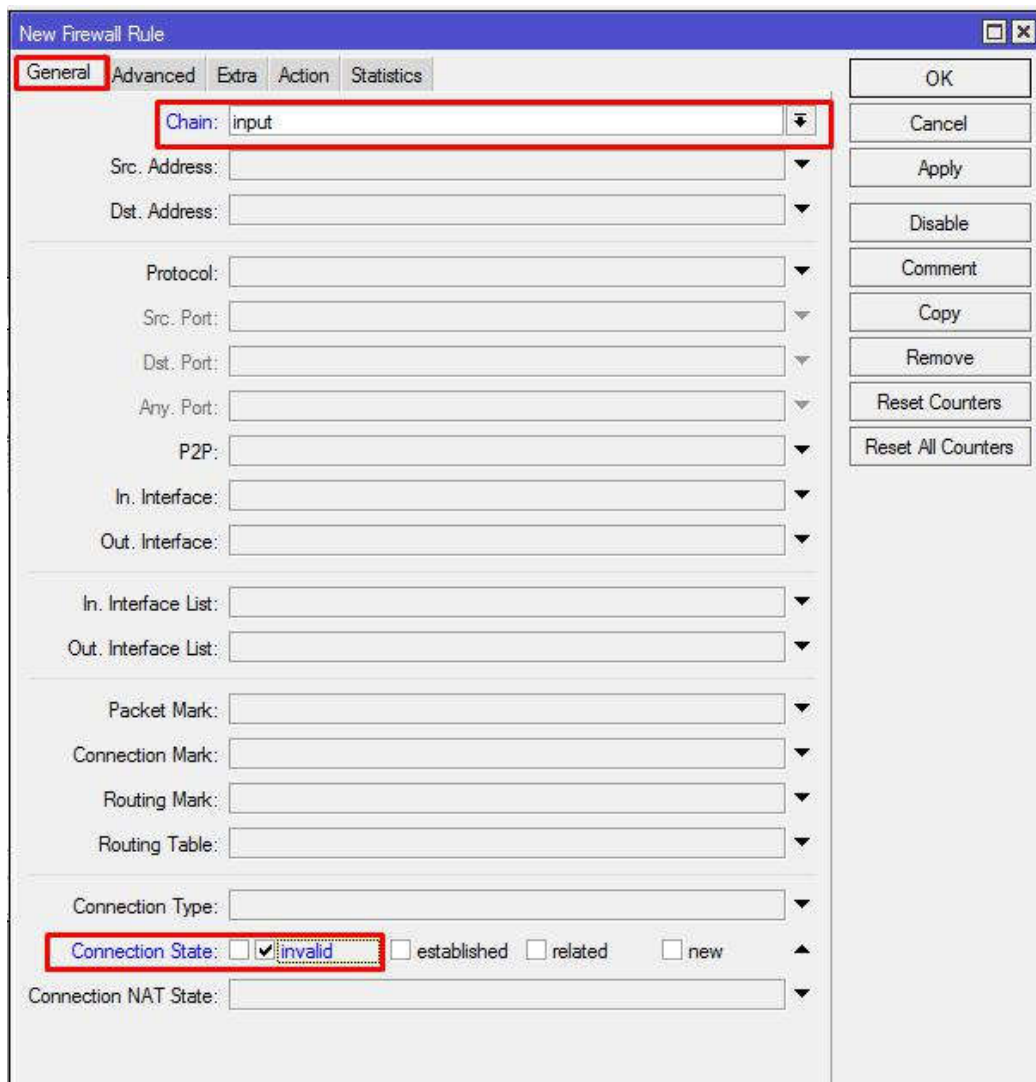
**Step by step :**

kita akan membuat 4 rule degan cara yang sama tetapi degan isi yang berbeda.

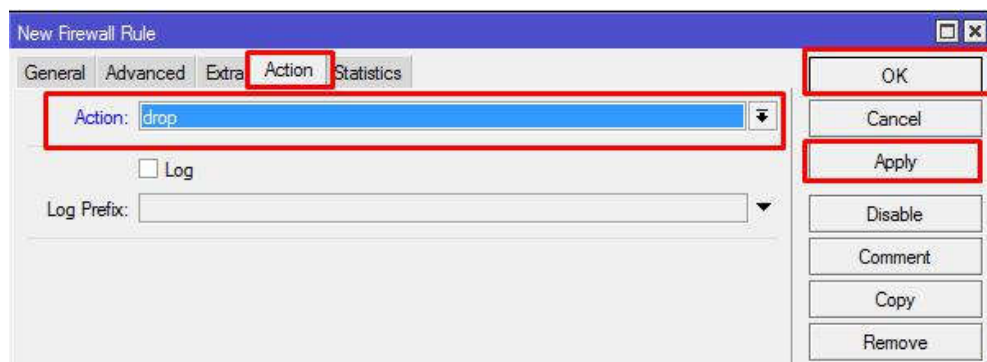
1. Kita akan coba terlebih dahulu membuat rule untuk connection state invalid drop, degan cara cari menu **IP>firewall>add(+)**



2. Lalu masuk ke tab general isi **chain=input** dan **connection state=invalid**



3. Setelah itu tinggal masuk ke tab action dan masukan **action=drop** setelah itu jangan di apply dan OK



4. Setelah itu buat 3 rule kembali dengan cara yang sama tetapi dengan isi yang berbeda, sebagai berikut :

**Connection state=estabilized dan action=accept**

**Connection state=related dan action=accept**

**Connection state=new dan action=passthrough**

Dan ketiga rule yang tadi menggunakan **chain=input**

5. Maka akan menghasilkan 4 rule dengan action drop, accept, accept, dan passthrough

Setelah kita buat 4 rule ini maka resource router kita dapat lebih hemat dari sebelumnya, dikarenakan proses filtering selanjutnya akan dilakukan ketika koneksi sudah berjalan

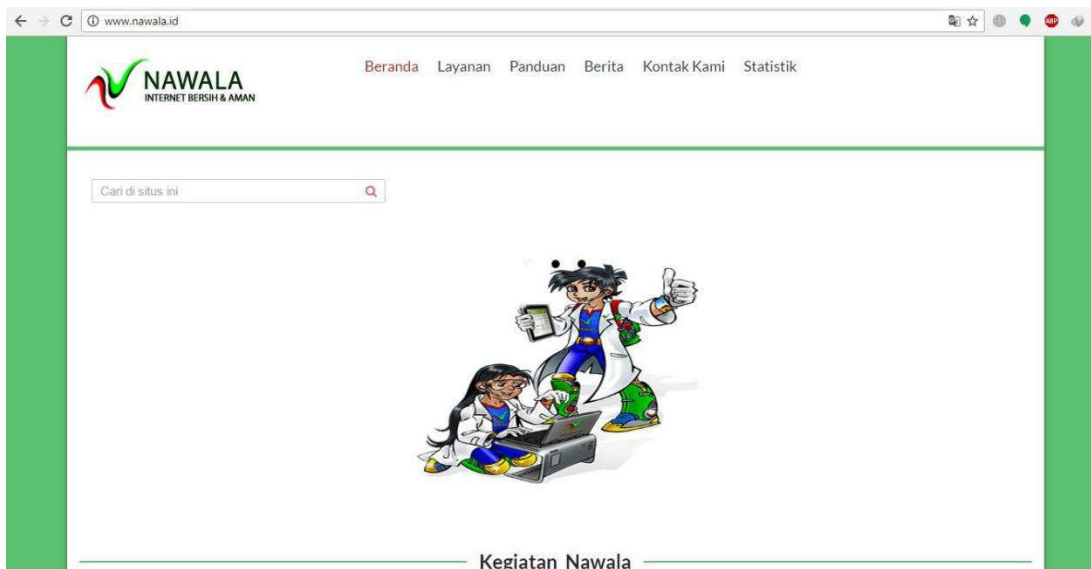
## LAB 21 Block Situs Porno Menggunakan Transparent DNS

Kita semua sekarang mengetahui bahwa dunia internet sekarang sudah menjadi teman sehari-hari dari semua kalangan, baik itu anak-anak sampai orang tua pun memanfaatkannya. Semuanya bisa mencari apa saja yang ada di internet dikarenakan internet itu sendiri super lengkap.

Banyak hal-hal yang dapat menambah wawasan tentang pembelajaran dan juga hal-hal positif lainnya, Namun tidak sedikit juga hal negatif yang akan didapatkan dari Internet, seperti halnya situs perjudian dan juga situs pornografi, dan yang semacamnya. Ada juga orang yang memang berniat jahat yang menampilkan situs pendidikan namun ketika di klik malah berubah menjadi situs pornografi. Bayangkan jika anak-anak yang membuka situs tersebut, mereka pun akan berpikir yang belum saatnya mereka pikirkan, dan juga bisa merusak masa depan mereka yang seharusnya mereka menjadi calon generasi masa depan kita.

Maka dari itu, kita sebagai orang yang tidak ingin hal itu terjadi harus mencegah hal tersebut, MikroTik pun menyediakan hal tersebut yaitu fitur Transparent DNS, dengan fitur tersebut kita bisa memblokir situs-situs yang berbau porno, perjudian, dll. Kali ini saya akan menggunakan suatu situs yang berfungsi untuk memblokir semua konten berbahaya itu, misalnya yang akan kita labkan kali ini ialah NAWALA. Jadi maksudnya yaitu, kita membuat peraturan bahwa bila ada client yang mencari situs porno maka akan dibelokkan jalurnya ke [www.nawala.id](http://www.nawala.id). Berikut caranya :

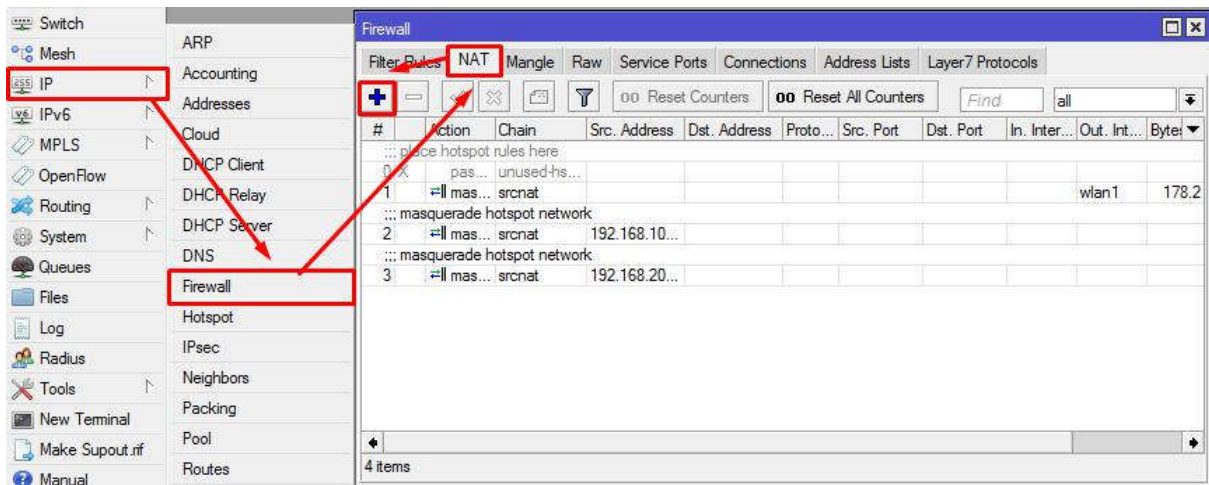
1. perlu diketahui, kita akan memblokir semua client yang terhubung ke router kita agar tidak mencari situs porno tersebut.
2. Koneksikan terlebih dahulu PC ke internet melalui routerboard kita.
3. Cari IP NAWALA terlebih dahulu di internet dengan memasukan [www.nawala.id](http://www.nawala.id), namun IP NAWALA yang saya dapatkan waktu itu adalah **202.125.83.14**



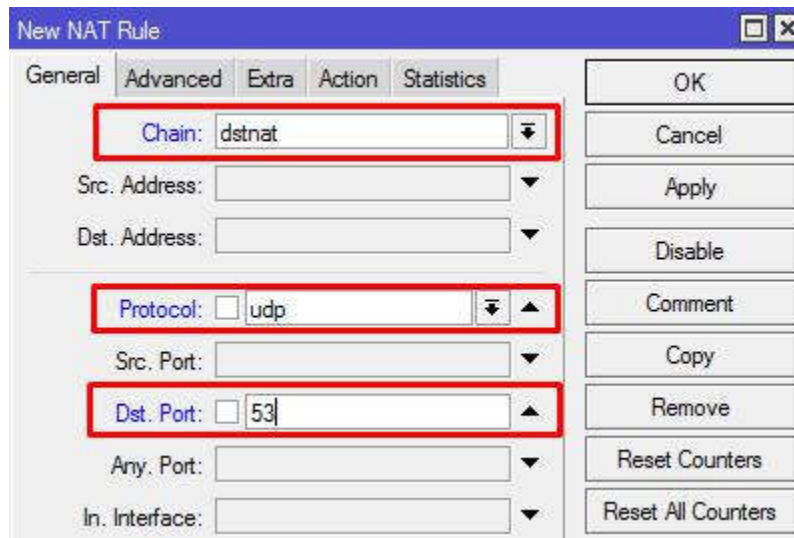
```
C:\Users\Lenovo>nslookup nawala.id
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: nawala.id
Address: 202.125.83.14
```

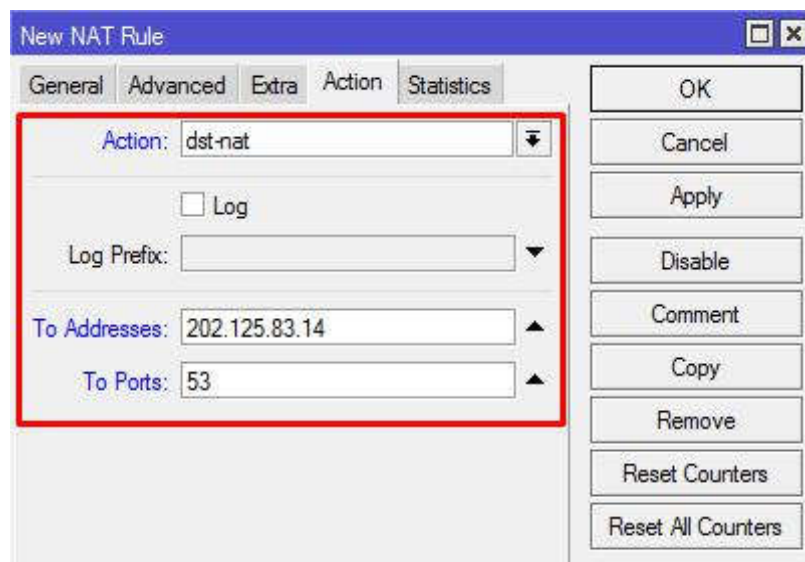
4. Kemudian login Winbox terlebih dahulu.
5. Masuk menu **IP > Firewall > NAT > Add**.



6. Pada tab **General** masukan **chain=dstnat**, **protocol=udp**, **dst. Port=53** (Port 53 adalah Port dari Domain Name System / DNS).



7. Pindah ke tab **action** > **action=dst-nat**, **to addresses= 202.125.83.14** (IP NAWALA), **to ports=53**.



8. Kemudian Apply dan OK.
9. Selanjutnya bisa di cek di browser, coba cari situs porno apapun, misalkan [www.playboy.com](http://www.playboy.com). maka jika transparent DNS kita berhasil akan seperti ini tampilannya.

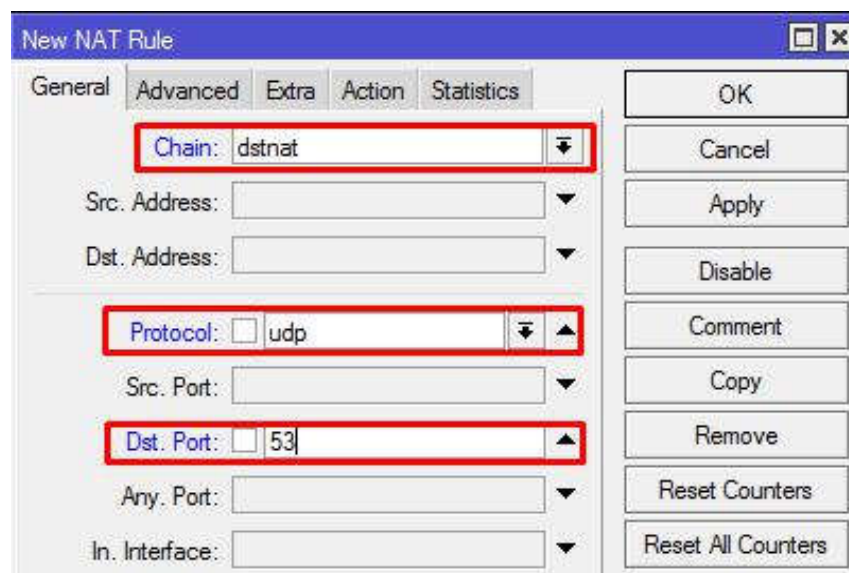




Catatan : apabila kita tidak diblokkan ke NAWALA nya sendiri malah ke Internet positif itu dikarenakan internet positif lebih dahulu memblok situs dibanding NAWALA.

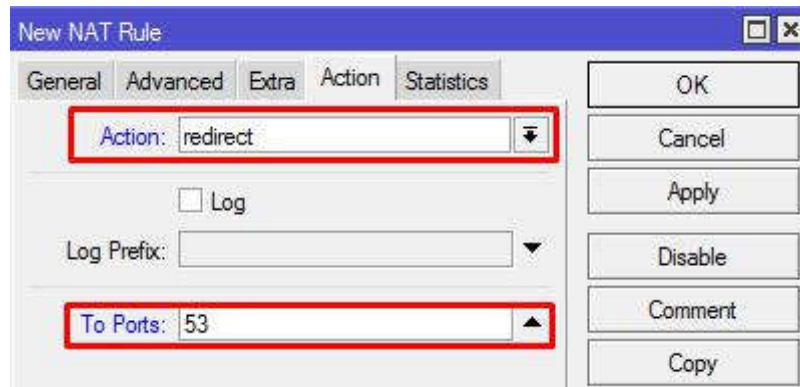
Itu adalah cara simple dari Transparent DNS, ada cara lain dengan maksud dan tujuan yang sama, cara kali ini kita mengkonfigurasi Transparent DNS tidak hanya di Firewall saja tetapi juga di menu DNS. Langsung saja kita coba.

1. Login Winbox terlebih dahulu.
2. Masuk ke menu **IP > Firewall > Add.**
3. Pada tab *General*, isikan **Chain=dstnat** lalu **Protocol=udp** dan **Dst.Port=53**.

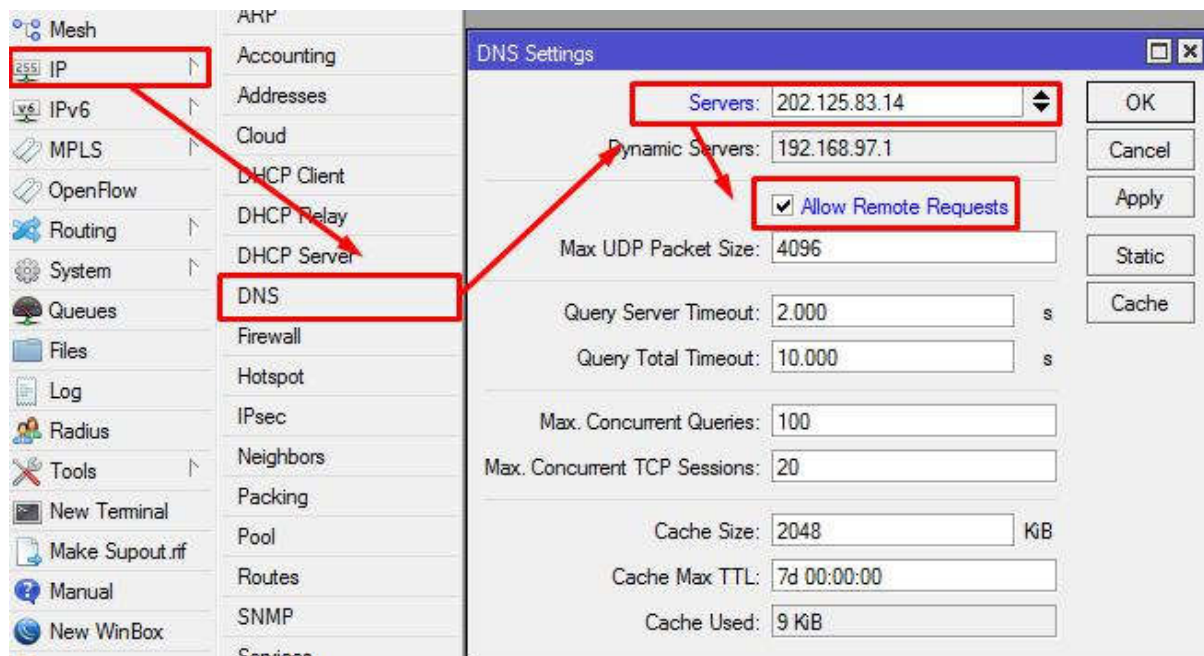


4. Kemudian jangan lupa untuk mengganti **Action** nya menjadi **redirect**.

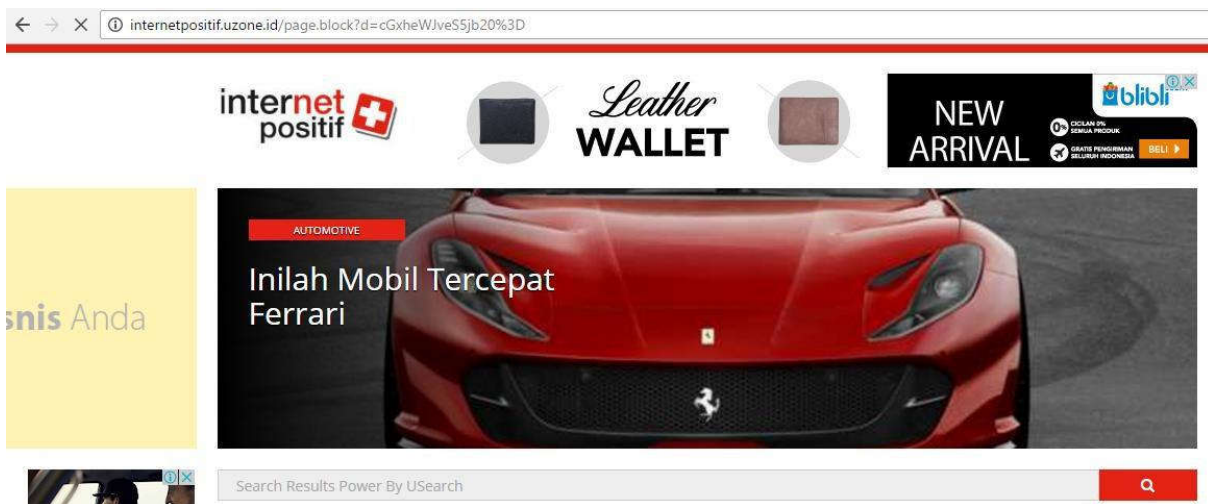
Dan juga isikan **To. Port=53**. Lalu Apply dan OK.



5. Setelah kita selesai dengan Firewall, sekarang kita pindah ke menu DNS di **IP > DNS** lalu isikan **Server=202.125.83.14** dan juga centanglah **Allow Remote Request** kemudian Apply dan OK.



6. Buka lagi suatu situs porno, dan lihat apakah bisa dibuka atau tidak?



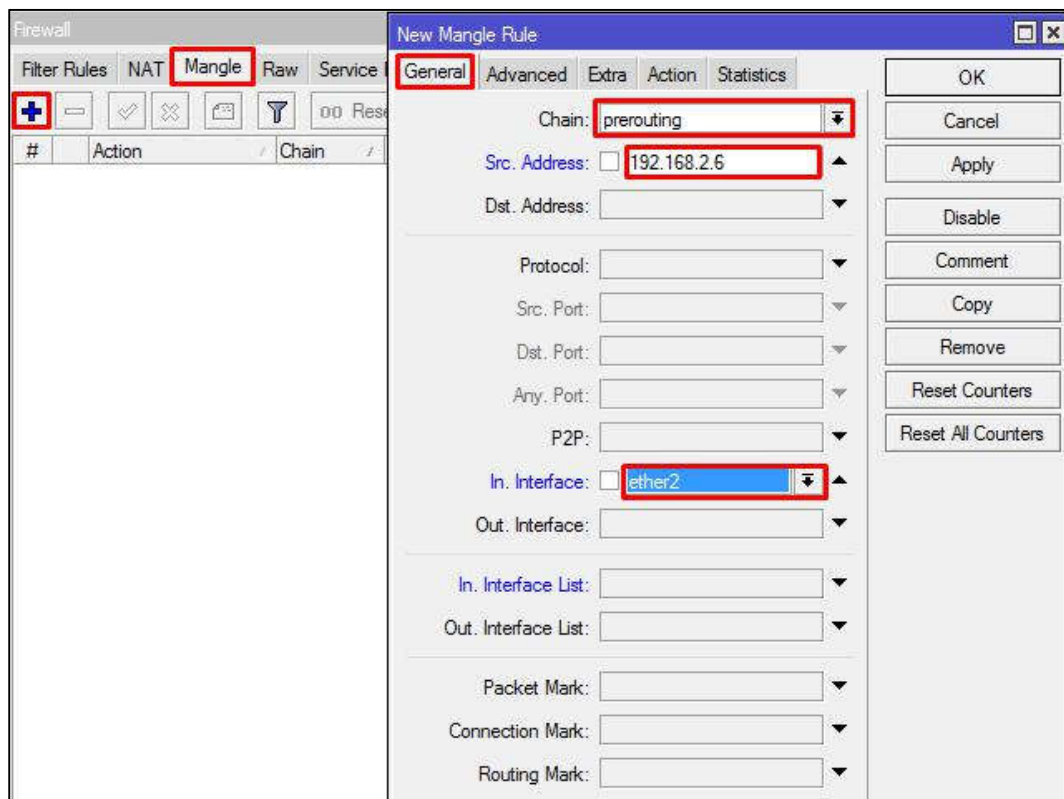
Kesimpulannya teknik ini merupakan salah satu teknik mudah untuk memblokir website yang bermuatan konten pornografi, perjudian, scam, dll. Dengan Open DNS Nawala kita tidak perlu susah payah memblokir satu persatu website pornografi Karena semua website yang bermuatan konten pornografi sudah dimasukkan kedalam database Nawala.

## LAB 22 Mangle

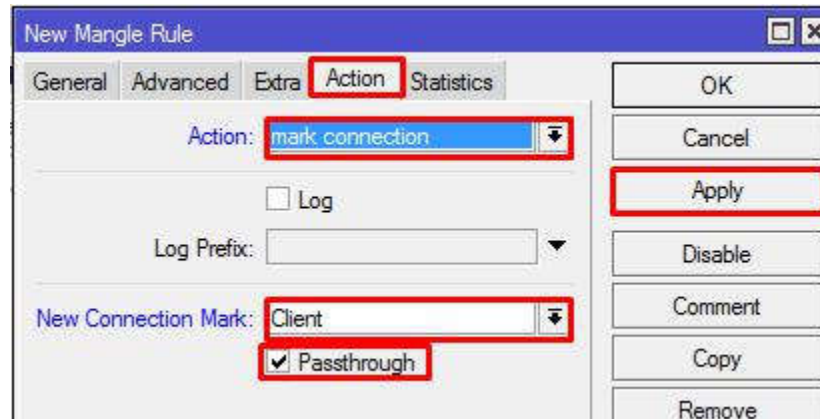
Di Lab kita akan membuat Rule Mangle untuk Queue, Rule Mangle berfungsi untuk menandai Paket (Marking) yang keluar masuk Router..jika kita menggunakan Mangle untuk Queue maka Kita bisa membatasi bandwidth Upload dan Download,dan kita juga bisa membatasi Bandwidth Per-Extensi (.MP3, .MKV) artinya jika kita melakukan Queue dengan menambahkan mangle maka kita bisa membatasi bandwidth secara Detail.. di lab ini kita akan mencoba membuat Mangle untuk traffic Upload dan Download...

Pertama kita akan membuat 1 rule mangle dengan menggunakan Action mark Connection yang berfungsi untuk menandai koneksi baru yang di buat oleh Client..

- Klik IP > Firewall > Mangle > Add (+)
- Isi Chain=Prerouting ,Src.Address=192.168.2.6 (IP Client) ,  
In.Interface=Ethenet2 (Mengarah ke Client)

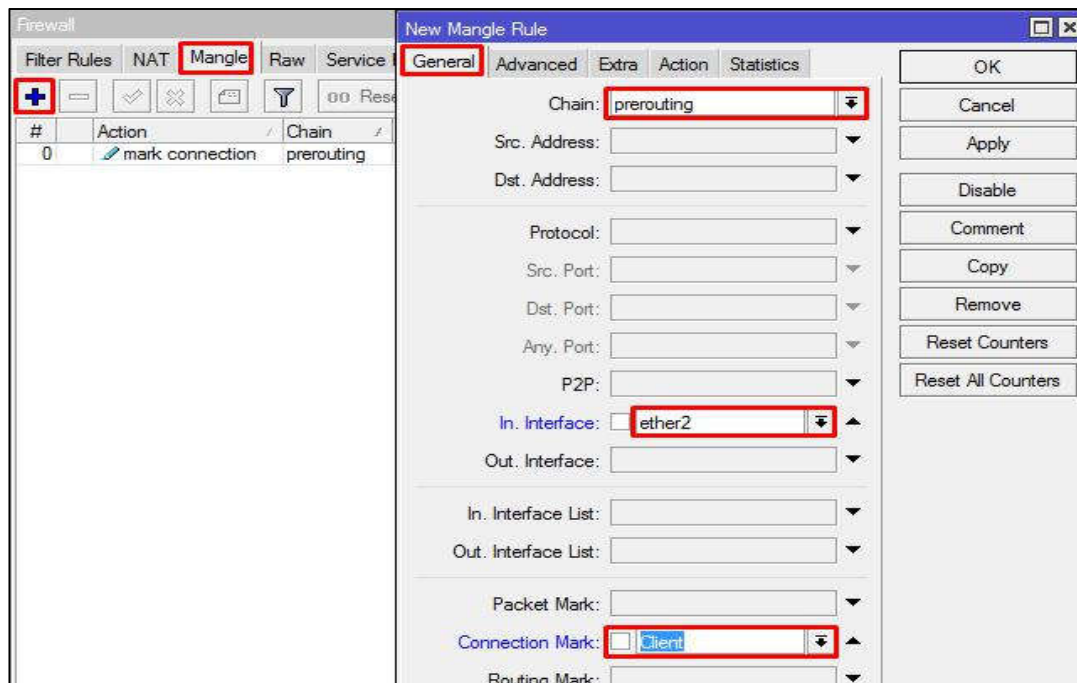


- Lalu Klik Action
- Isi Action=Mark Connection ,New Connection Mark=Client (bebas) ,  
Checklist Passthrough
- Lalu Apply dan OK



Jika kita sudah menandai koneksi koneksi baru yang di buat Oleh Client ,selanjutnya kita akan membuat rule mangle untuk Menandai Packet Upload dan Download..

- Klik IP > Firewall > Mangle > Add (+)
- Isi Chain=Prerouting , Connection Mark=Client In.Interface=Ethenet2 (Mengarah ke Client)

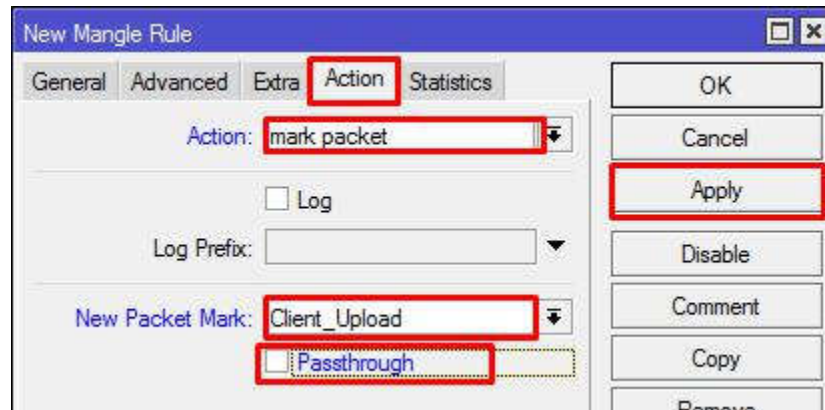


- Lalu Klik Action
- Isi Action=Mark Packet ,New Connection Mark=Client\_Upload (bebas)



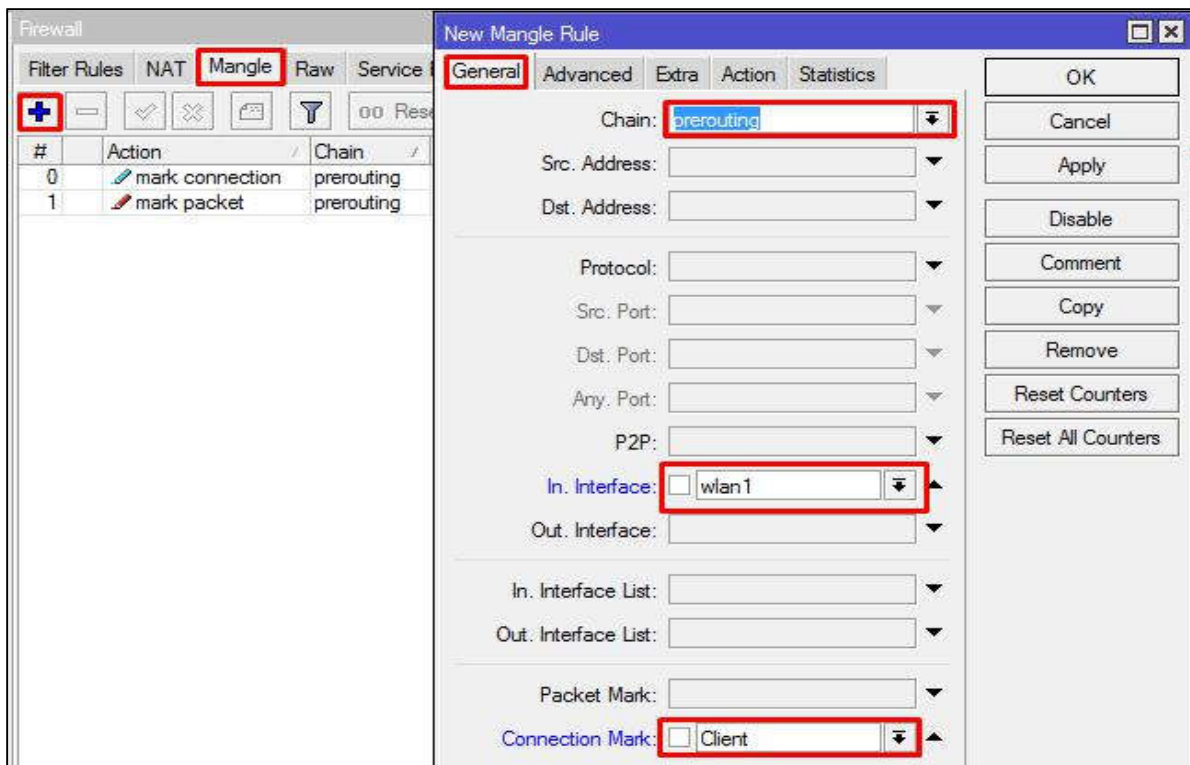
,Unchecklist Passthrough

- Lalu Apply dan OK



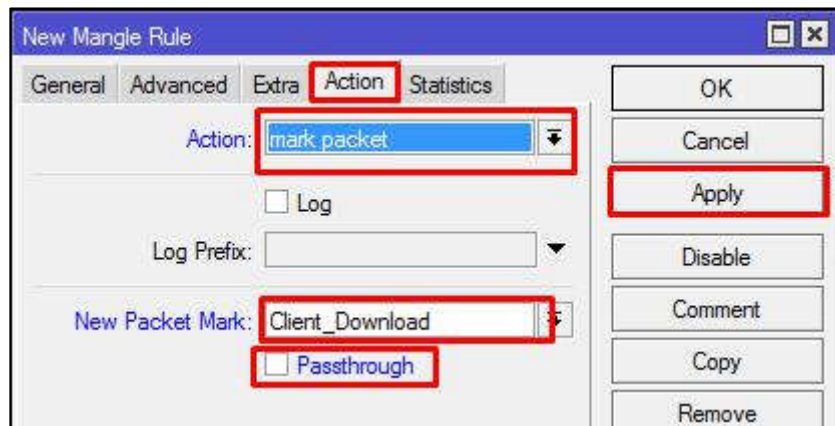
Rule di atas adalah Rule untuk Upload Client,selanjutnya kita akan membuat Rule mangle untuk Download Client..

- Klik IP > Firewall > Mangle > Add (+)
- Isi Chain=Prerouting , Connection Mark=Client, In.Interface=Wlan1 (mengarah ke Internet)



- Lalu Klik Action
- Isi Action=Mark Packet,New Connection Mark=Client\_Download (bebas)  
,Unchecklist Passthrough
- Lalu Apply dan OK





Jika sudah Membuat 3 Rule tersebut maka Trafic Upload dan Download Client akan tercatat...