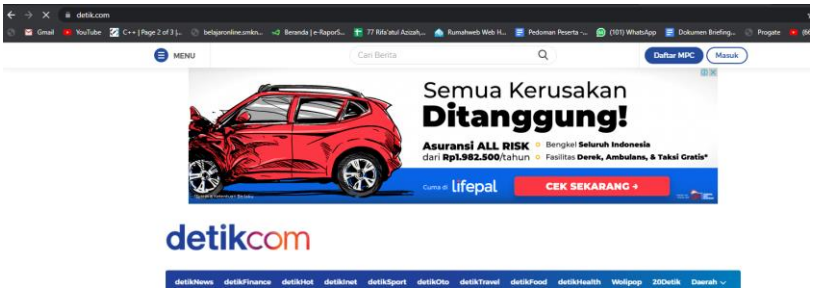
BLOKIR SITUS

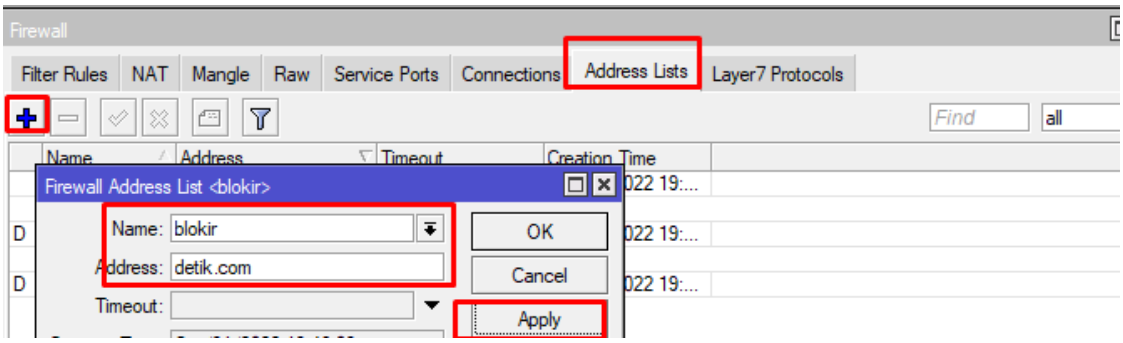
ADDRESS LIST, LAYER 7 PROTOKOL

Disini kita akan mensimulasikan untuk pengamanan jaringan local, yang memiliki akses keluar (internet).

1. Menggunakan Address List
   a. Blokir situs detik.com, pastikan situs detik.com bisa diakses terlebih dahulu

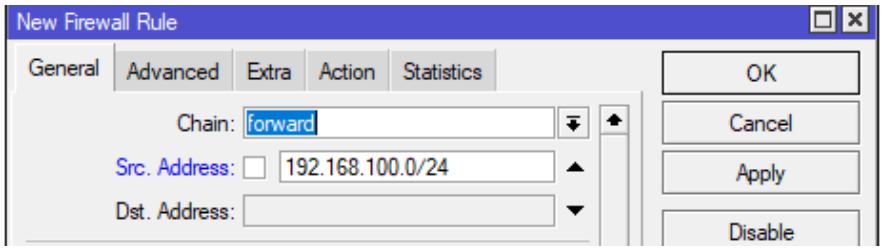


Buat address lists untuk situs yang akan diblokir dengan nama blokir

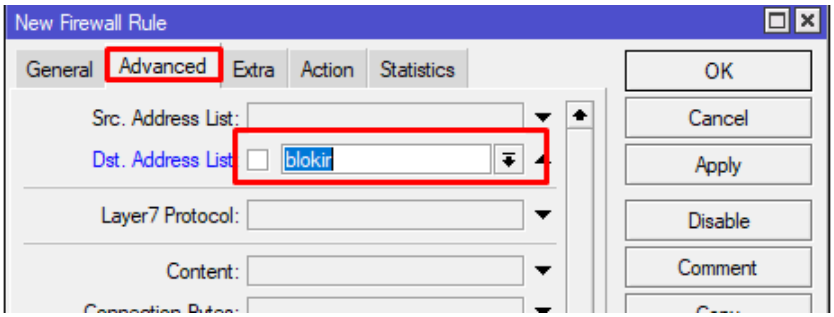


Tambahkan filter rule nya, chain = forward, dst address = “nama address list yang sudah dibuat”, action = drop

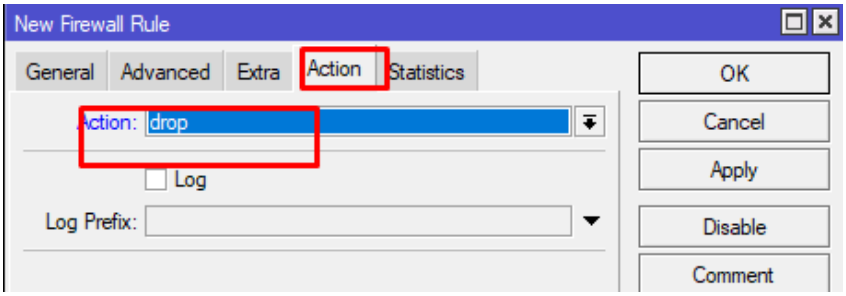
Pada tab general src.address adalah ip yang akan melakukan request akses, jika satu jaringan yang akan dilakukan blokir maka isikan network nya.



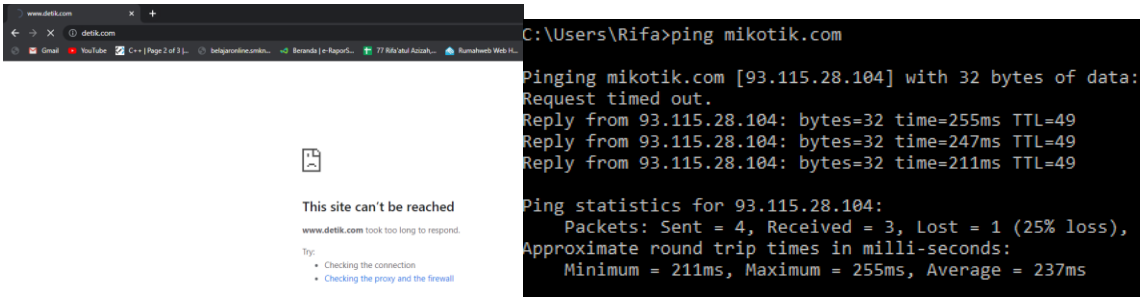
Pada tab advanced, dst.address adalah nama address list yang sudah didaftarkan sebelumnya, yang mana berisi address dari situs detik.com



Kemudian pada tab action = drop

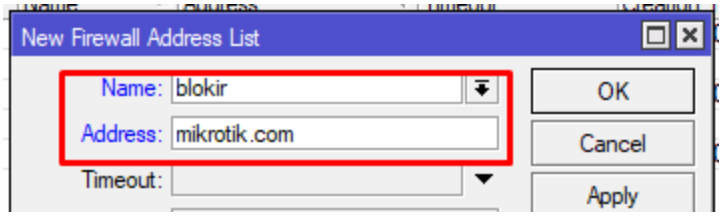


Lakukan pengecekan, apakah situs detik.com sudah berhasil terblokir



Jika akan menambahkan situs yang akan diblokir, bisa dimasukkan melalui address list.

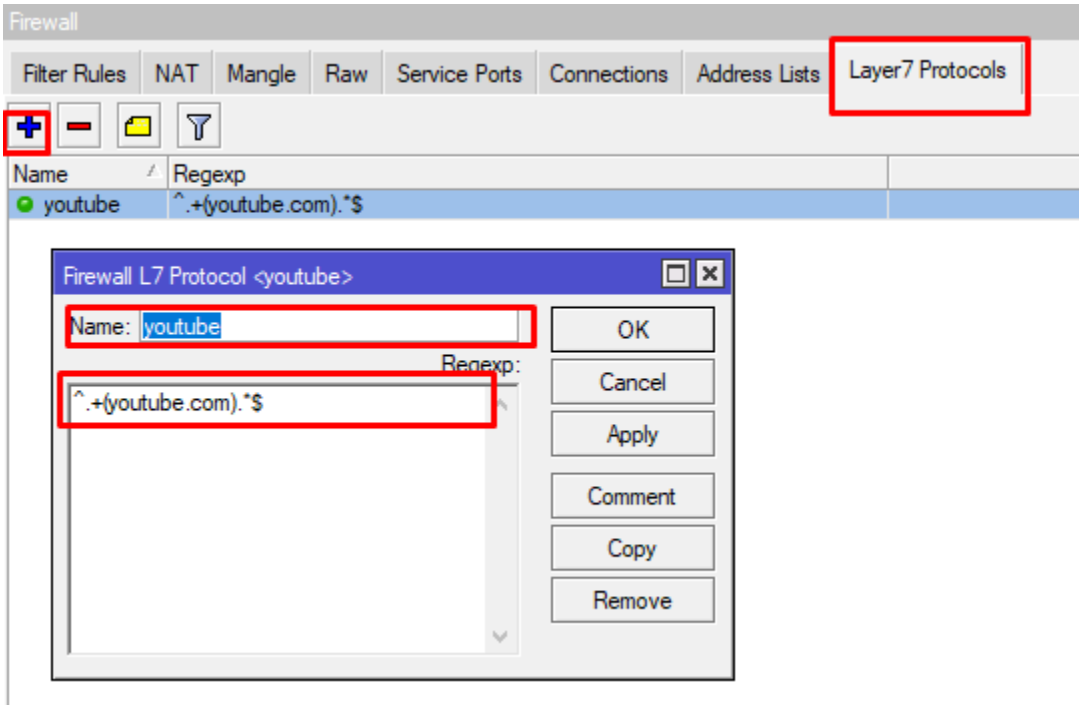
Contoh: menambahkan situs mikrotik.com



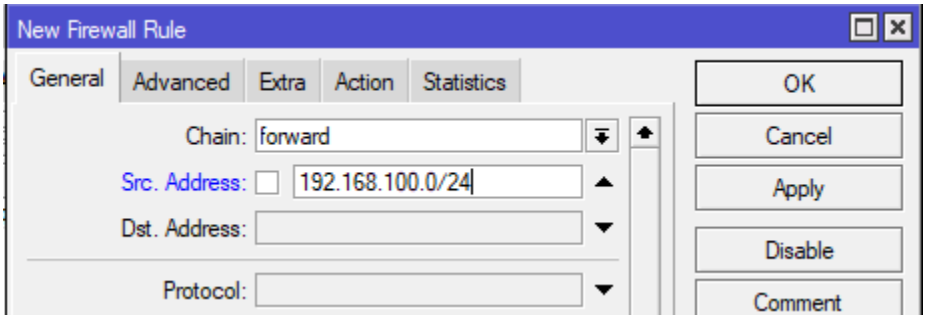
Selanjutnya silahkan melakukan blokir untuk 2 situs, yaitu situs web SMKN 1 Doko dan youtube.

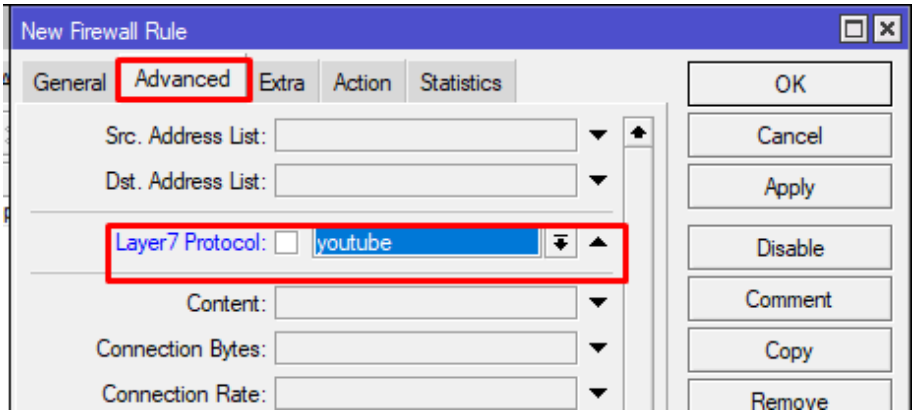
2. Menggunakan layer 7 protokol

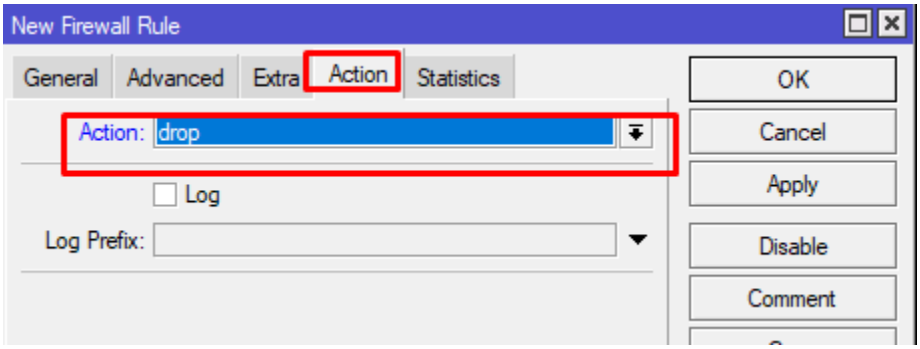
Layer 7 Protocol adalah metode pencarian pola terhadap paket data yang melewati jalur **ICMP, TCP dan UDP**. Firewall layer 7 merupakan firewall yang sangat bagus dan komples dibandingkan firewall – firewall lain yang ada pada MikroTik. Beberapa service dan protocol yang berada di layer 7 ini misalnya **HTTP, FTP, SNTP**, dan lain-lain.



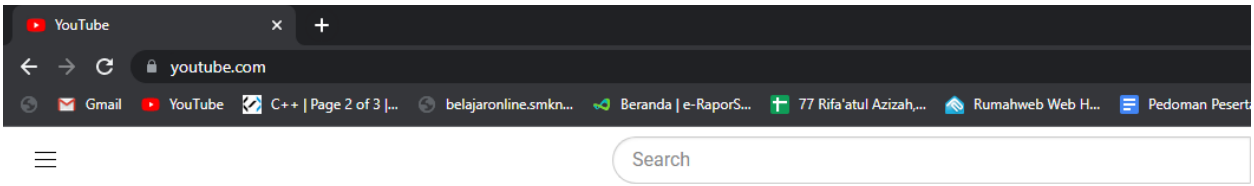
Tambahkan kode regexp, Regular Expression (REGEX) adalah konstruksi bahasa untuk mencocokkan teks berdasarkan pola tertentu, terutama untuk kasus-kasus kompleks. Contoh misalkan mencari teks berawalan karakter tertentu, memiliki jumlah perulangan dari suatu teks, dan lain sebagainya.







Selanjutnya cek apakah situs berhasil terblokir




```
C:\Users\Rifa>ping youtube.com
Ping request could not find host youtube.com. Please check the name and try again.
```

Tugas selanjutnya adalah :

Lakukan blokir terhadap situs

1. Facebook.com
2. Twitter.com
3. Blokir untuk download file dengan ekstensi .mp3

NAT(NEWORK ADDRESS TRANSLATION)

srcnat dan dstnat

srcnat

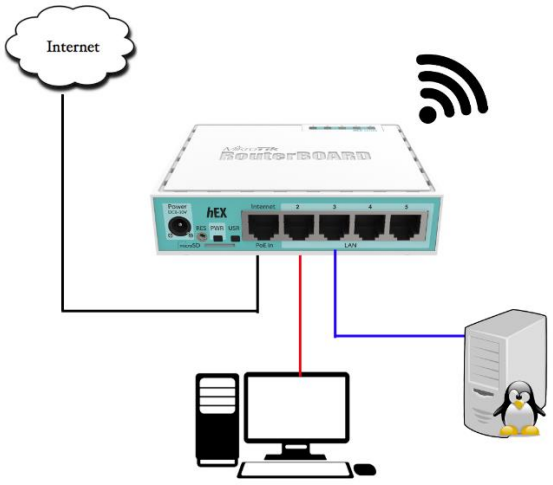
SrcNAT (Source NAT) adalah protokol pengalihan yang dijalankan oleh router untuk paket yang berasal dari jaringan private ke jaringan publik. Dalam protokol SrcNAT, sebuah paket data akan diubah source addressnya menjadi IP publik agar bisa diterima oleh komputer tujuan.

dstnat

DstNAT (Destination NAT) adalah proses pengubahan alamat IP tujuan dari website/IP publik ke alamat IP komputer yang mengakses website tersebut. Tujuan DstNAT adalah agar PC lokal dapat menerima data yang berasal dari IP Publik.

Perbedaan	**srcnat**	**dstnat**
Arah paket data	IP private ke Publik	Ip Public ke Ip Private
Cara kerja	Mengubah IP Sumber ke ip public	Mengubah IP tujuan ke ip Private
Metode	masquerading	Port forwading, transparent proxy, port mapping

Topologi



Ketentuan:

1. Ether1 ke Internet = dhcp client
2. Ether2 ke Jaringan Lokal = dhcp server
3. Ether3 ke server Debian = static
4. Wlan/hotspot = dhcp server

   IP Ether 1 = dhcp client

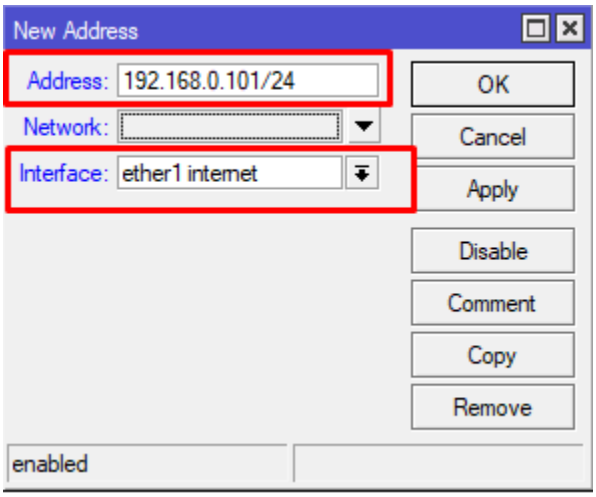
   IP Ether 2 = 192.168.100.1/24

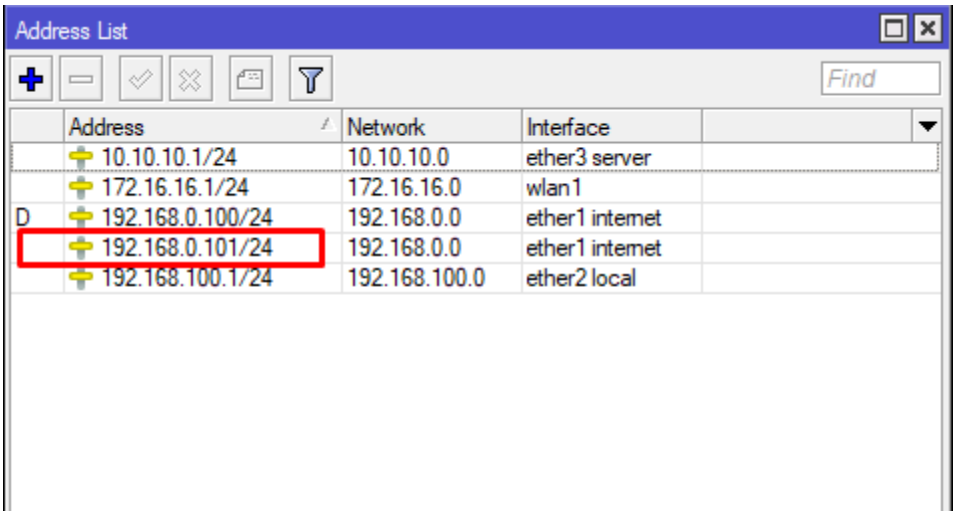
   IP Ether 3 = 10.10.10.1/24

   IP Wlan = 172.16.16.1/24
5. Pastikan semua mendapat akses internet (client local, server, wlan)
6. Install aplikasi webserver pada server Debian (apache2)

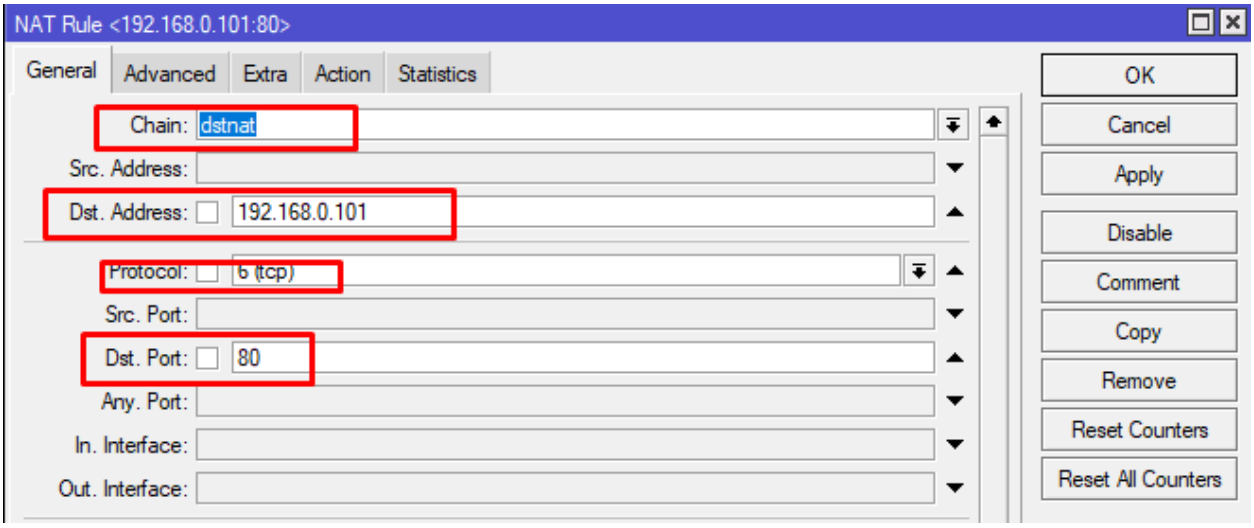
Langkah-langkah:

1. Pada server Debian lakukan installasi apache dan pastikan apache dapat berjalan
2. Tambahkan ip public yang nantinya akan kita pinjam untuk mengakses web server yang ada pada jaringan local



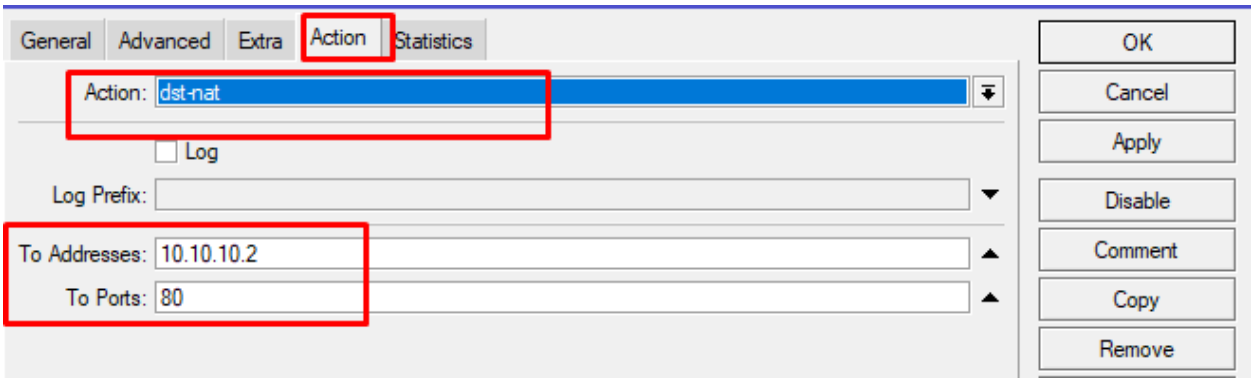


3. Tambahkan rule untuk **dstnat** dengan tujuan alamat ip public dapat diubah menjadi ip private, sehingga web dari server local dapat diakses. Pada tab general isikan rule sperti berikut



Dst.address adalah alamat ip public yang kita tambahkan tadi, nantinya akan kita manfaatkan untuk mengakses web server dari computer di jaringan public.

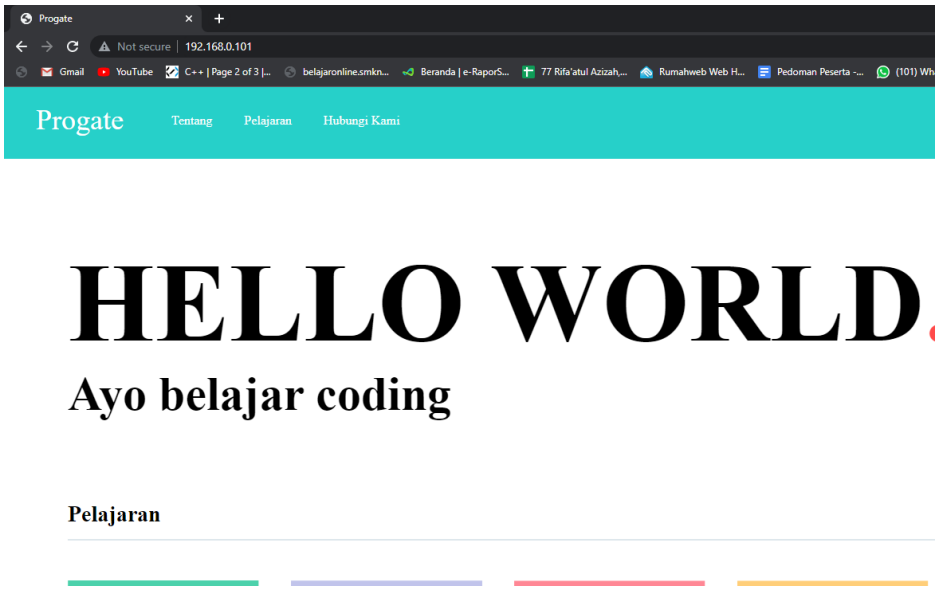
Pada tab action isikan rule seperti di bawah, to address adalah alamat dari server local.



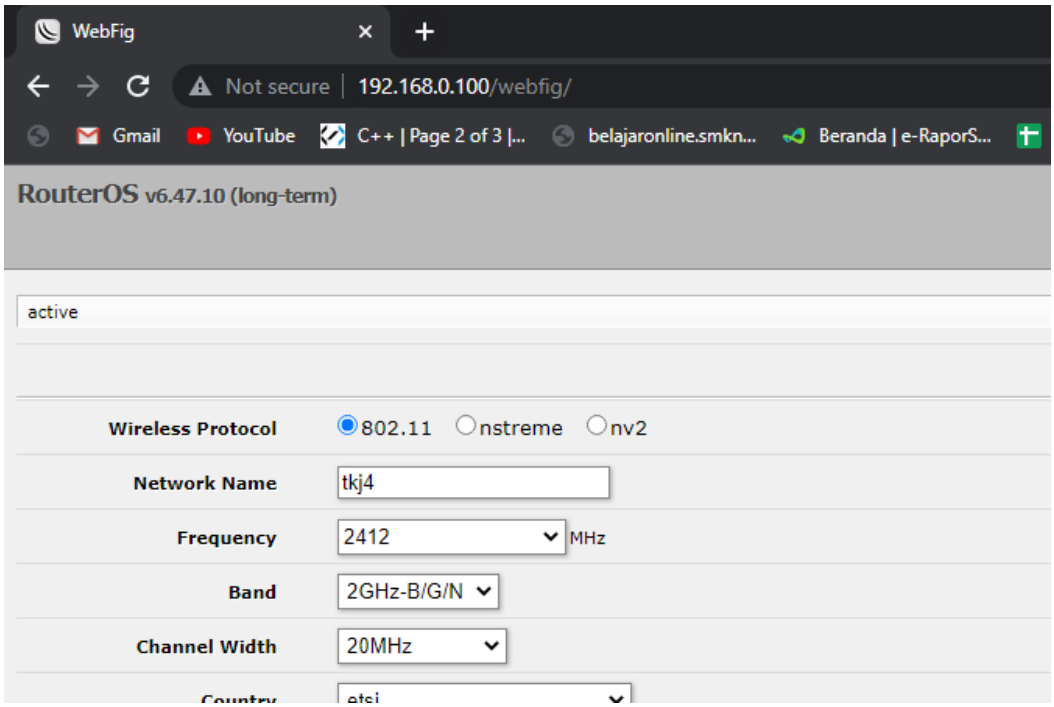
4. Pengujian

Akses webserver menggunakan ip public yang sebelumnya yaitu 192.168.0.101, melalui:

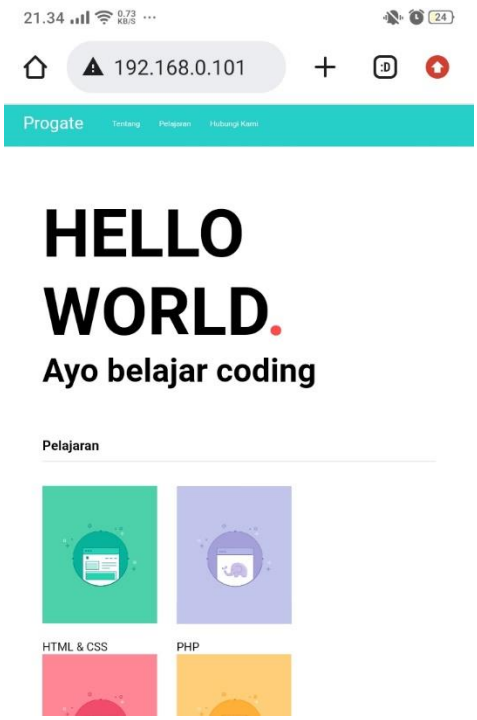
a. Computer client/local



Jika akses 192.168.0.100 maka akan diarahkan ke webfig


WebFig
Not secure 192.168.0.100/webfig/
Gmail
YouTube
C++ | Page 2 of 3 |...
belajaronline.smkn...
Beranda | e-RaporS...
RouterOS v6.47.10 (long-term)
active
Wireless Protocol
802.11
nstreme
nv2
Network Name
tkj4
Frequency
2412
MHz
Band
2GHz-B/G/N
Channel Width
20MHz

b. Wlan


192.168.0.101
Progate
HELLO
WORLD.
Ayo belajar coding
Pelajaran
HTML & CSS
PHP