Modul
Mendesain Sistem Keamanan Jaringan
(Menggunakan Mikrotik)

Oleh:

M. Saiful Mukharom, S.Kom., MTCNA., MTCRE.

Pendahuluan

- Pengantar

  Modul ini mengulas dan membahas materi kompetensi keahlian Mendesain Sistem Keamanan Jaringan, pada kurikulum KTSP 2006 ini di ajarkan di kelas XII TKJ semester I, Mengingat minimnya materi mengenai kompetensi keahlian ini (sepengetahuan kami) maka kami mencoba untuk mengulas lebih mendalam, Insya Allah.

  Materi akan kami usahakan dibahas dengan kondisi nyata, bismillah kami usahakan. Modul ini akan keluar dua versi yaitu Modul yang sasarannya umum dan modul yang sasarannya pelajar SMK (yang kami lengkapi dengan indikator dan lembar kegiatan). Yang menarik dari modul ini adalah pembahasannya lebih pada kenyataan dan banyak praktiknya.

- Petunjuk

  Simulasi untuk melakukan lab pada modul kali ini sebagian menggunakan terminal dan sebagian menggunakan GUI. Selanjutnya desainlah sendiri topologi tersebut(direkomendasikan), Karena ketika topologi didesain dengan system yang berbeda akan menyebabkan tidak berjalannya topologi.

  Beberapa materi akan ada yang kami arahkan ke alamat peramban internet, yang sekiranya tidak memungkinkan dibahas dimodul ini.

- Requirements

Skill

- Pengetahuan dasar network fundamental
- Materi MTCNA
- Kebiasaan Ngonfig
- Terbiasa edit preferences dan config di gns3 (jika ada kendala jangan sungkan-sungkan menanyakan ke kami)

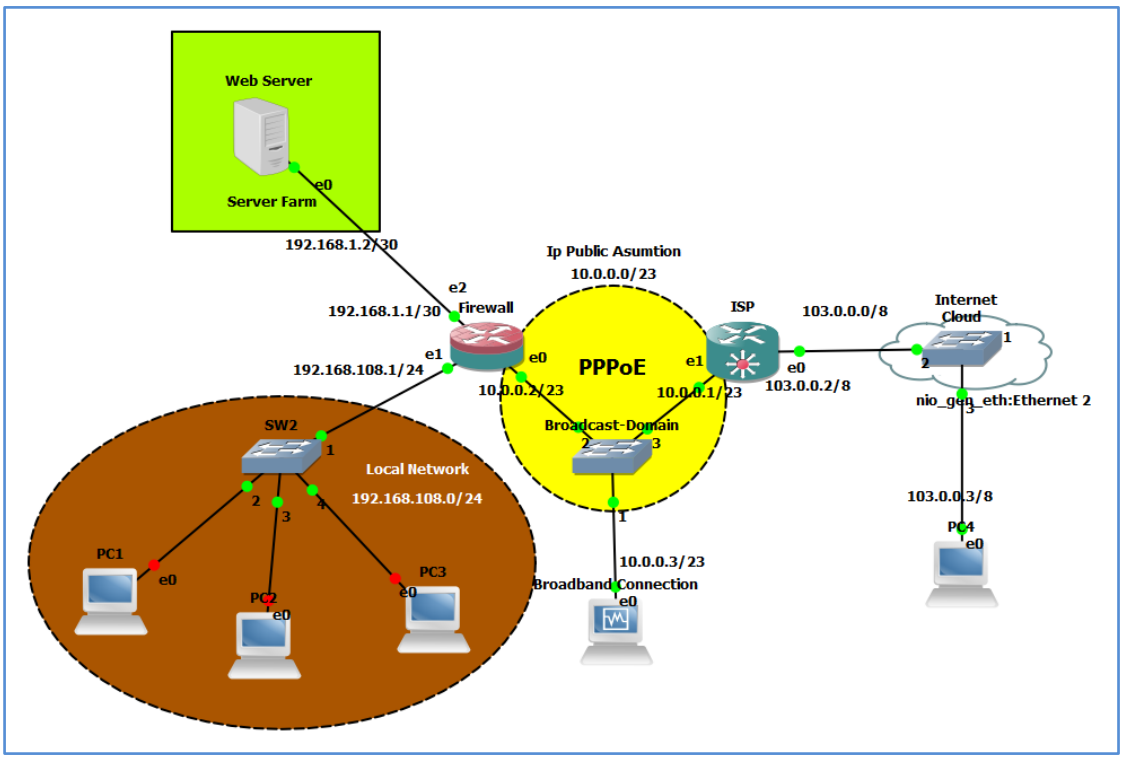
Aplikasi

- GNS3 Versi 1.3.9 atau yang lebih baru
- CHR-6.34.4.img
- VirtualBox-5.2 atau yang lebih baru

Hardware

- Komputer atau Laptop sepesifikasi minimal ram 4 GB, Processor Support VT(Biasanya perlu setting di BIOS untuk enable support VT)

- Skenario Topologi



- Penjelasan Singkat Skenario Topologi

  Alur dari Skenario ini adalah diawali dengan menyiapkan ip loopback(sebagai penghubung antara host machine dengan gns3) kemudian dilanjutkan dengan menambahkan cloud yang dihubungkan dengan router ISP dan VPCS(Client Jalur langsung ke internet, ini ditandai dengan device yang terhubung melalui modem USB) dengan bantuan Switch(beralasan karena tidak bisa router ISP link langsung ke cloud), dilanjutkan dengan desian router firewall dan Broadband Connection, Router Firewall akan digunakan sebagai pengaman jaringan local seperti melakukan src-nat dan dst-nat, bloking host dari mengakses internet jika melakukan ping ke firewall dan seterusnya.

  Topologi yang kami desain bersumber dari ISSA Journal – The Principles of Network Security Desain yang di tulis oleh Mariusz Stawowski, intinya topologi yang kami desain mengambil dari referensi jurnal tersebut, meskipun tidak sedetail yang dibahas pada journal.

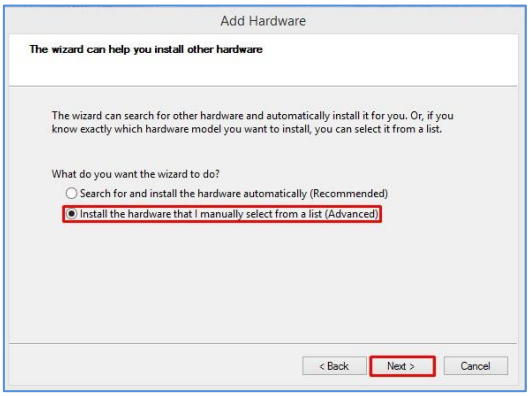
- Tujuan

  Siswa dapat memahami topologi desain keamanan jaringan lebih nyata.

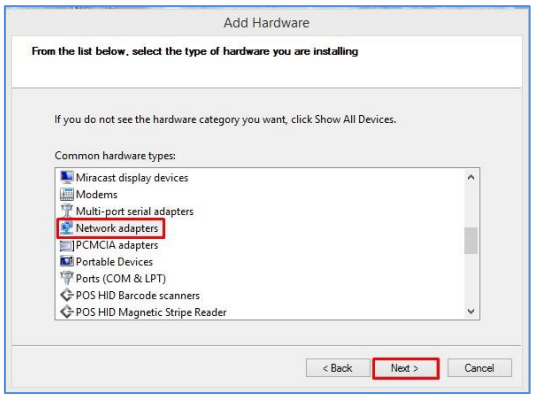
- Persiapan

  Instalasi IP Loopback

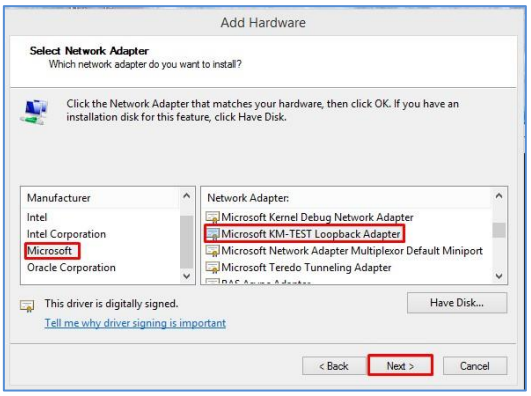
a. Jalankan CMD Run as Administrator, kemudian ketikkan perintan "hdwwiz", maka akan muncul seperti menu diatas.



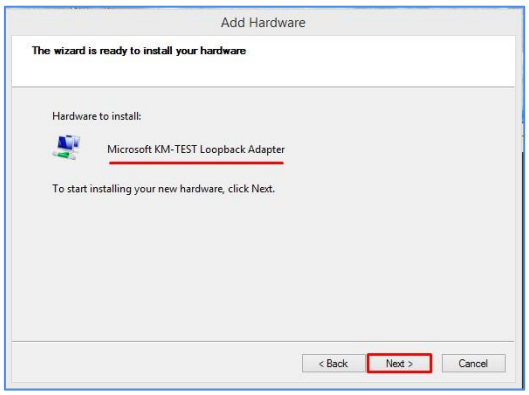
b. Pilih radio button "install the hardware that I manually select from a list(Advanced)".

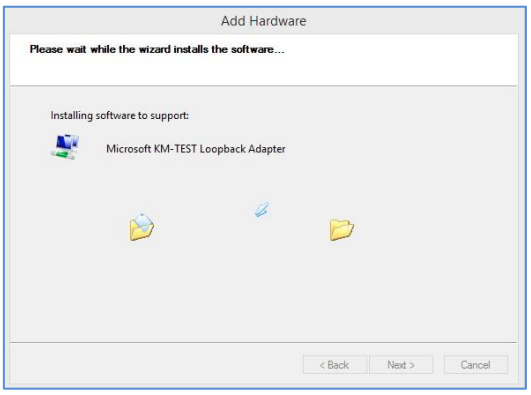


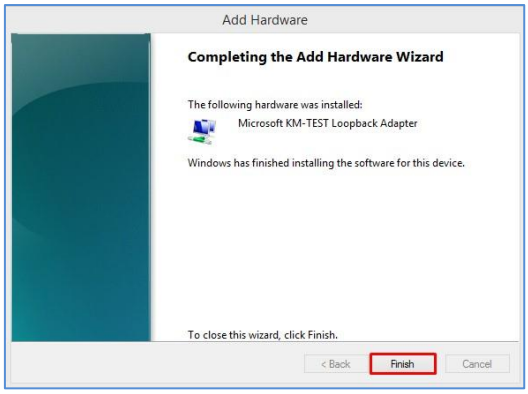
c. Pilih [Network adapter], Kemudian [Next]

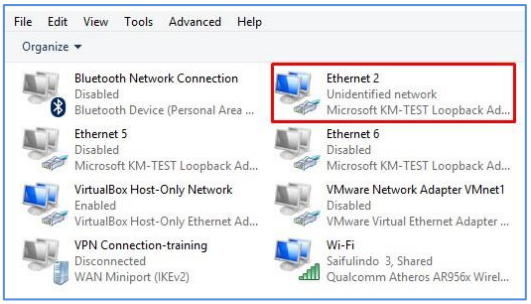


d. Pilih [Microsoft], Kemudian [Microsoft KM-Test Loopback Adapter], Berikutnya [Next].









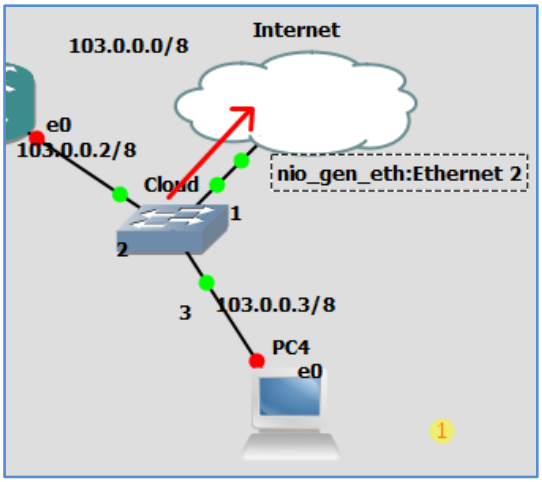
Jika telah selesai instalasi "add hardware" maka akan muncul adapter seperti gambar diatas.

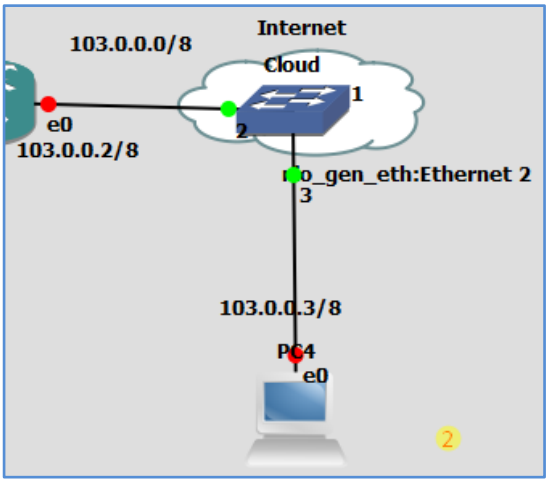
- Instalasi gns3
  Untuk melakukan instalasi gns3 sudah sangat gamblang penjelsannya di https://www.gns3.com/support/docs/, minimal konfigurasi seperti install gns3 di berbagai sistem operasi, edit preference, menambahkan IOS Images, dll.
- Desain Jaringan
  Tonton Videonya di alamat:

Modul I

Persiapan

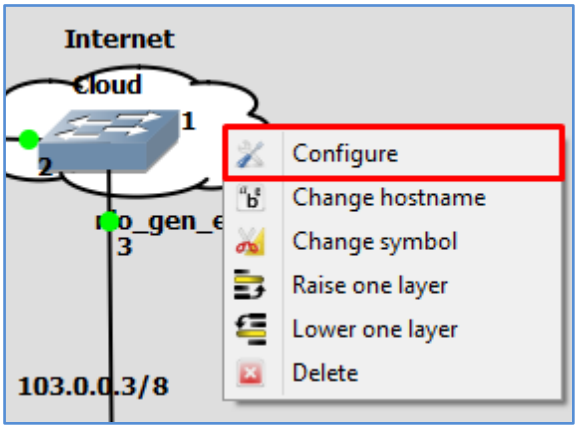
- Topologi IP Loopback

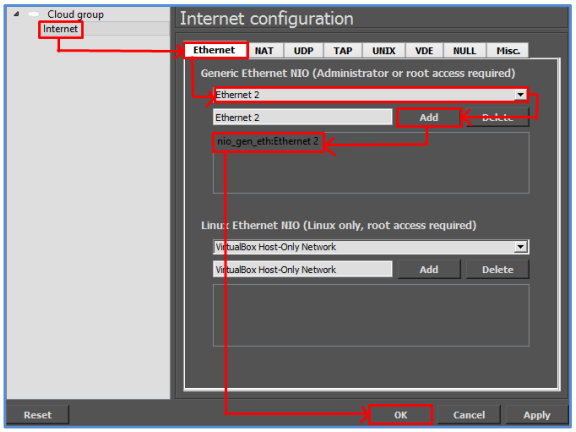




IP Loopback akan dihubungkan dengan cloud, keterangan tambahan lain: device yang terhubung dengan cloud maka, harus melewati perangkat switch dahulu, gambar 1 dan 2 menjelaskan bahwa switch di geser ke arah cloud adalah agar rapi saja.

- Menambah port loopback di cloud

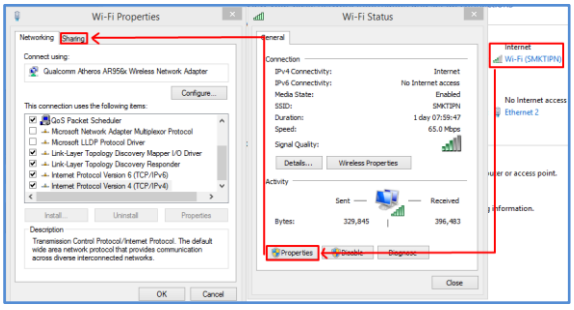


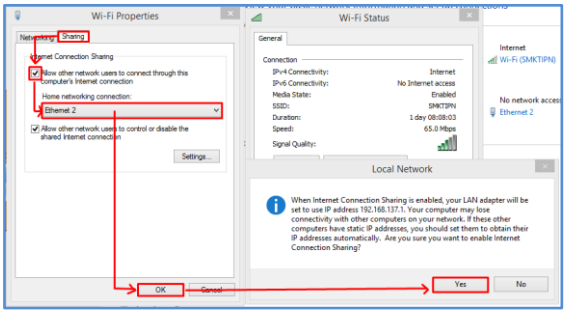


Klik kanan pada simbol awan, pilih [Configure], tambahkan ethernet 2 yang merupakan representasi dari IP Loopback.

- Share Internet

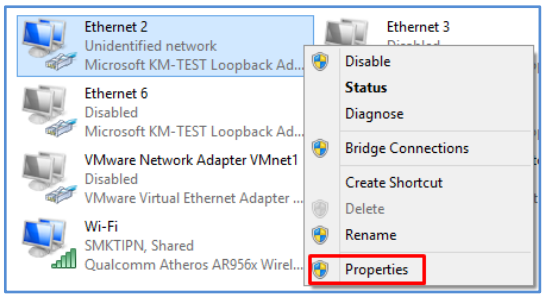
Sharing internet dari Adapter Wifi atau Lokal Network ke IP Loopback.



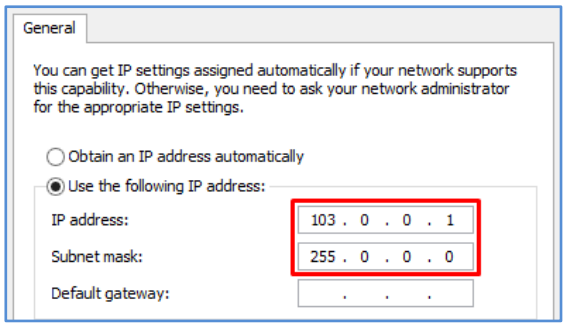


Ketika akses internet di share ke Loopback maka adapter tersebut akan berubah IP-nya secara otomatis menjadi 192.168.137.1/24(ini tidak mengapa), tinggal nanti diganti lagi IP-nya menjadi 103.0.0.1/8 (dan internet akan tetap ter-share).

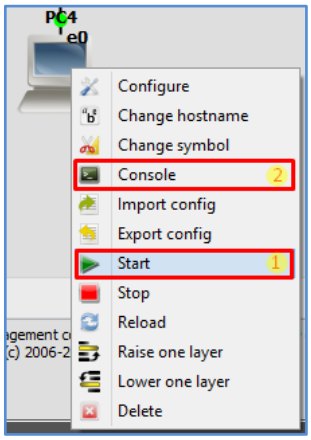
- Konfigurasi IP Address.
  - Loopback Komputer Host Machine



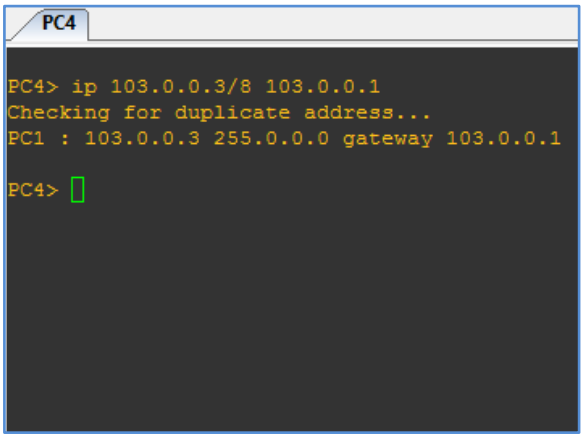
Klik kanan Network Adapter, Klik [Properties].



- PC4

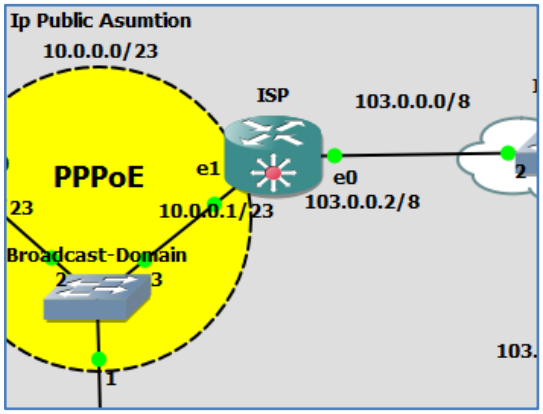


Klik kanan pada symbol pc4, pilih [Start], kemdian [Console]

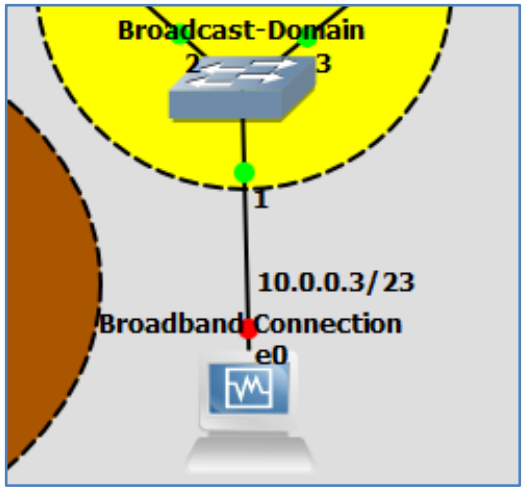


Command untuk mendaptkan ip Address secara automatis.

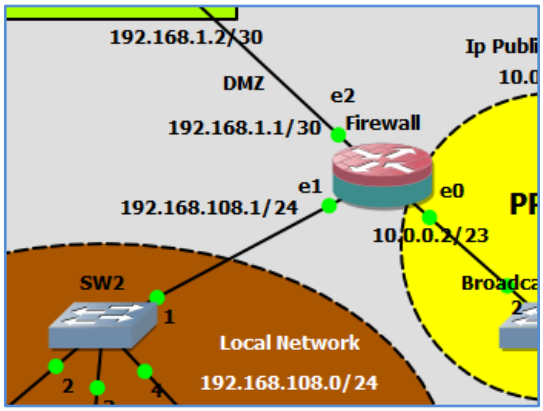
- Topologi



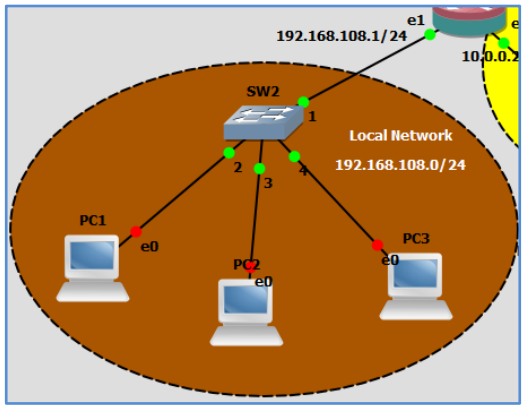
Posisi ISP



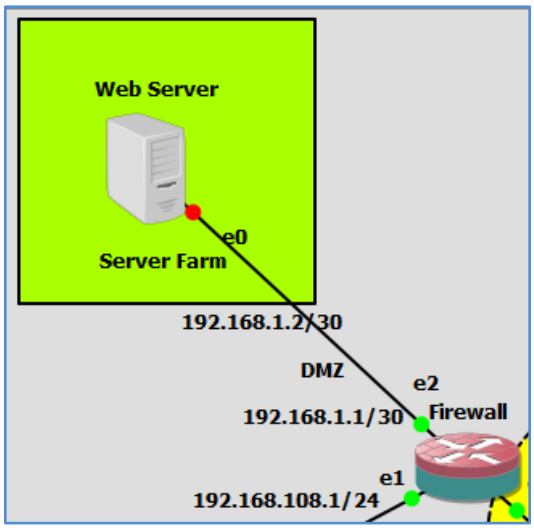
Posisi Broadband Connection



Posisi Firewall



Posisi Local Network



Posisi Server Farm

- ISP

```
[admin@ISP] > ip dns static add name=www.google.com address=10.0.0.1
[admin@ISP] > ip dns static pr
```

Config ether1

```
[admin@ISP] > ip address add address=103.0.0.2/8 interface=ether1
[admin@ISP] > ip address pr
```

Config ether2

```
[admin@ISP] > ip address add address=10.0.0.1/23 interface=ether2
[admin@ISP] > ip address pr
```

- Client Broadband Connection

  IP Address: 10.0.0.3/23

  Gateway: 10.0.0.1

  DNS: 10.0.0.1,8.8.8.8

- Firewall

  Config ether1

```
[admin@ISP] > ip address add address=10.0.0.2/23 interface=ether1
[admin@ISP] > ip address pr
```

Config ether2

```
[admin@ISP] > ip address add address=192.168.108.1/22 interface=ether2
[admin@ISP] > ip address pr
```

Config ether3

```
[admin@ISP] > ip address add address=192.168.1.1/30 interface=ether3
[admin@ISP] > ip address pr
```

Config DHCP

```
[admin@ISP] > ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: ether2
Select network for DHCP addresses

dhcp address space: 192.168.108.0/24
Select gateway for given network

gateway for dhcp network: 192.168.108.1
Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.108.2-192.168.108.254
Select DNS servers

dns servers: 10.0.0.1,8.8.8.8
Select lease time

lease time: 10m
[admin@ISP] > ip dhcp-server pr
```

- PC local network

  Config PC1, PC2 dan PC3

```
PC1> ip dhcp
DDORA IP 192.168.108.254/24 GW 192.168.108.1
```

```
PC1> sh ip

NAME        : PC1[1]
IP/MASK     : 192.168.108.254/24
GATEWAY     : 192.168.108.1
DNS         : 10.0.0.1
DHCP SERVER : 192.168.108.1
DHCP LEASE  : 597, 600/300/525
MAC         : 00:50:79:66:68:00
LPORT       : 10006
RHOST:PORT  : 127.0.0.1:10007
MTU:        : 1500

PC1> ping www.google.com
```

Config Server Farm

```
Ubuntu-server login: smkti
Password: @smkti
smkti@ubuntu-server:~$ sudo nano /etc/network/interfaces
auto eth0
iface eth0 inet static
       address 192.168.1.2
       netmask 255.255.255.252
       gateway 192.168.1.1
ctrl+O [Untuk simpan]
ctrl+X [untuk hapus]
smkti@ubuntu-server:~$ sudo bash
password: @smkti
root@ubuntu-server:~$ ifdown -a && ifup -a
root@ubuntu-server:~$ ping 192.168.1.1
```

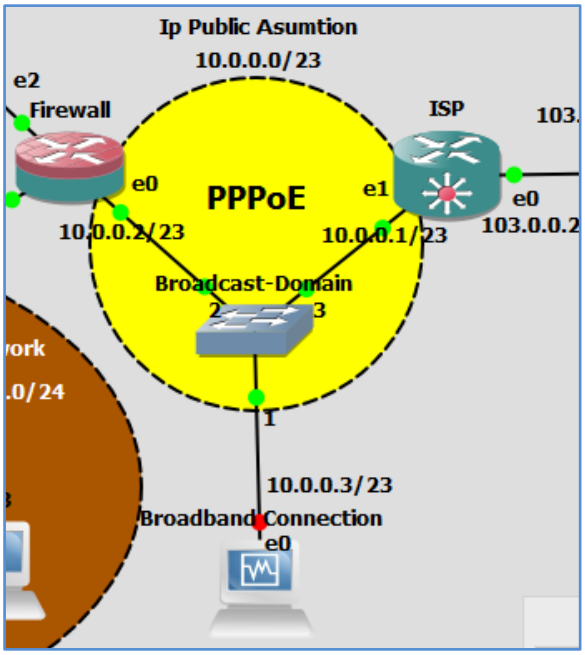
- Penjelasan

  Pada tahapan persiapan ini hanya melakukan konfigurasi IP Address saja. Selebihnya nanti akan di bahas dimodul ini, jadi tidak lebih dari persiapan saja.

Modul II

PPPoE

- Topologi



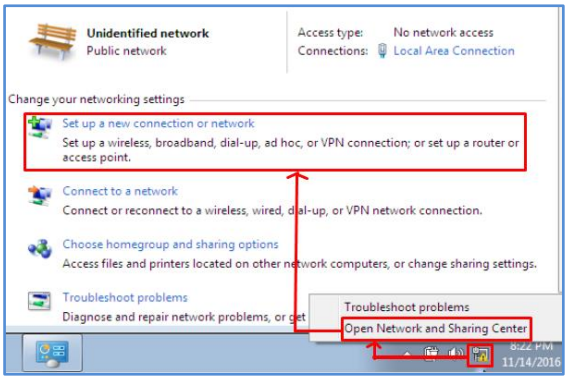
- Config

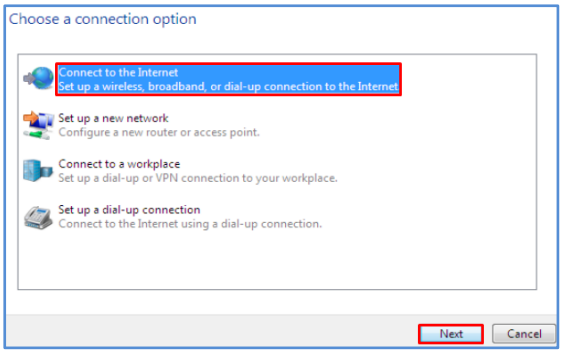
  ISP

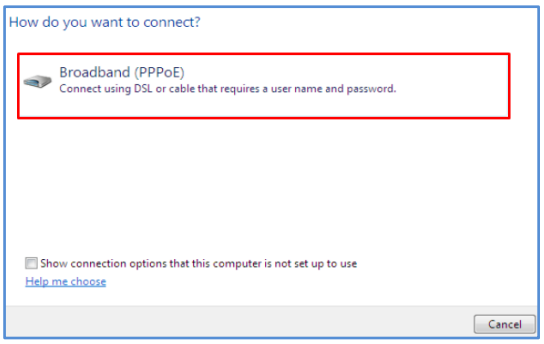
  Membuat PPPoE Server

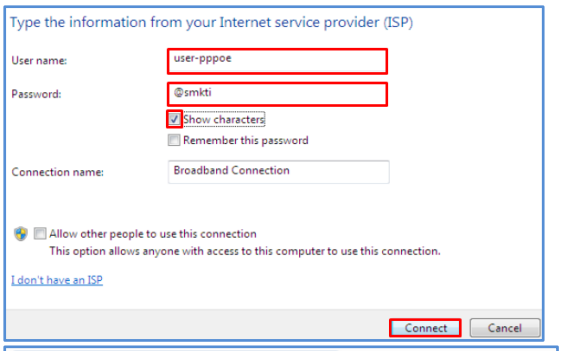
```
[admin@ISP] > ip dns add servers=10.0.0.1,8.8.8.8
[admin@ISP] > ip route add dst-address=0.0.0.0/0 gateway=103.0.0.1
[admin@ISP] > interface pppoe-server server add service-name=service-pppoe interface=ether2
keepalive-timeout=900000
[admin@ISP] > ip pool add name=pool-pppoe-client ranges=10.0.0.2-10.0.0.10
[admin@ISP] > ppp secret add name=user-pppoe password=smkti
[admin@ISP] > ppp profile set default local-address=10.0.0.1 remote-address=pool-pppoe-
client dns-server=10.0.0.1,8.8.8.8
[admin@ISP] > ping google.com
```

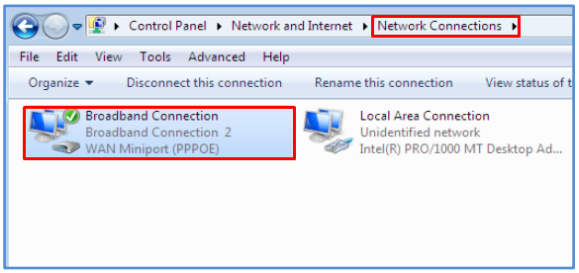
  Broadband Connection

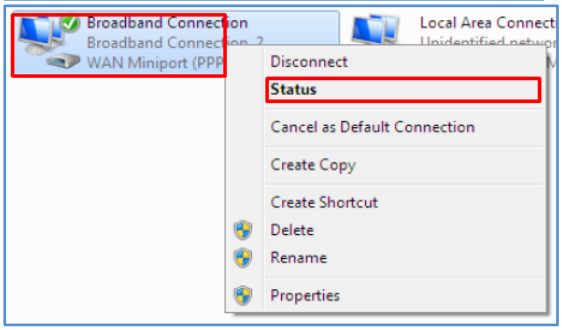


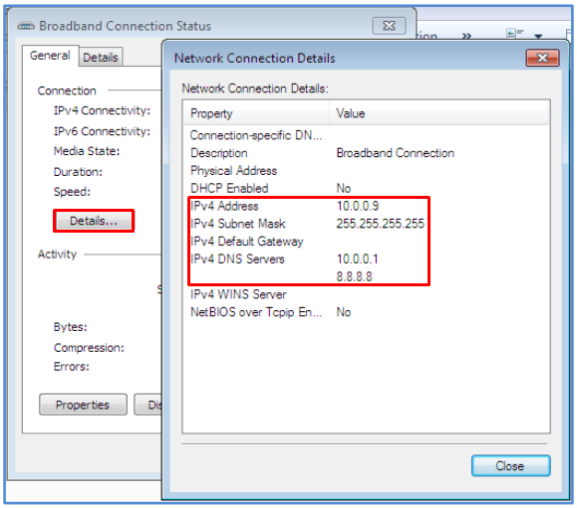












Firewall

```
[admin@Nama-Kalian] > interface pppoe-client add interface=ether1 user=user-pppoe
password=@smkti use-peer-dns=yes
[admin@Nama-Kalian] > interface pppoe-client pr
[admin@Nama-Kalian] > interface pppoe-client monitor pppoe-out2
          status: connected
          uptime: 12m27s
    active-links: 1
        encoding:
    service-name: service-pppoe
         ac-name: ISP
          ac-mac: 00:00:AB:76:70:01
             mtu: 1480
             mru: 1480
   local-address: 10.0.0.9
  remote-address: 10.0.0.1
-- [Q quit|D dump|C-z pause]
[admin@Nama-Kalian] > ip dns pr
                servers:
       dynamic-servers: 10.0.0.1,8.8.8.8
  allow-remote-requests: no
    max-udp-packet-size: 4096
   query-server-timeout: 2s
    query-total-timeout: 10s
              cache-size: 2048KiB
```

```
          cache-max-ttl: 1w
             cache-used: 9KiB
[admin@Nama-Kalian] > ip route add dst-address=0.0.0.0/0 gateway=10.0.0.1
[admin@Nama-Kalian] > ping google.com
[admin@Nama-Kalian] > ip address disable numbers=0
```

- Penjeasan

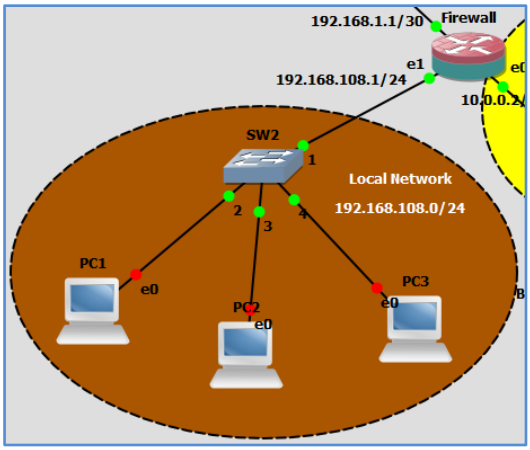
  PPPoE tidak membutuhkan ip address pada interface masing-masing device yang terhubung ke PPPoE Server, jadi PPPoE Client akan mencari(dial-up) sendiri, apakah dalam satu broadcast domain ini ada PPPoE Server. Anda bisa juga menggunakan fasilitas scan pada fitur PPPoE Client, yaitu seperti "`[admin@Nama-Kalian] > interface pppoe-client scan interface=ether1`". Dan pastikan antar PPPoE Client bisa saling ping. Jadi PPPoE ini membuat jalur tunnel(terowongan) sendiri dalam satu broadcast domain melalui ethernet(numpang jalur).

  Tambahan: Kemudian pastikan pada Broadband Connection IP Address juga di kosongi pada local area conection, jadi dapat IPnya dari PPPoE Server.

Modul III

Address List

- Topologi



- Config
  - Firewall

Deskripsi config:

1. Jika klient ping ke gateway maka di drop, tetapi tetap bisa ping ke www.google.com ataupun google.com (Hapus rule jika sudah berhasil)
2. Jika klient ping ke gateway maka di masukkan ke Address List, Siapapun yang terdaftar ke Address list maka nggak bisa akses www.google.com ataupun google.com, tetapi bagi siapa saja yang tidak ping ke gateway akan tetap dapat akses internet.

Set DNS-Server DHCP

```
[admin@Nama-Kalian] > ip dhcp-server network set dns-server=10.0.0.1,8.8.8.8 numbers=0
```

NAT

```
[admin@Nama-Kalian] > ip firewall nat add chain=srcnat action=masquerade out-
interface=pppoe-out2
```

Sekenario 1: Blok Akses ICMP

```
[admin@Nama-Kalian] > ip firewall filter add chain=input action=drop protocol=icmp in-
interface=ether2
```

Pengujian

```
PC1> ip dhcp
DORA IP 192.168.108.254/24 GW 192.168.108.1

PC1> sh ip

NAME         : PC1[1]
IP/MASK      : 192.168.108.254/24
GATEWAY      : 192.168.108.1
DNS          : 10.0.0.1  8.8.8.8
DHCP SERVER  : 192.168.108.1
DHCP LEASE   : 594, 600/300/525
MAC          : 00:50:79:66:68:00
LPORT        : 10006
RHOST:PORT   : 127.0.0.1:10007
MTU:         : 1500
```

```
PC1> ping www.google.com
www.google.com resolved to 10.0.0.1
84 bytes from 10.0.0.1 icmp_seq=1 ttl=63 time=34.150 ms
84 bytes from 10.0.0.1 icmp_seq=2 ttl=63 time=29.706 ms
84 bytes from 10.0.0.1 icmp_seq=3 ttl=63 time=30.338 ms
84 bytes from 10.0.0.1 icmp_seq=4 ttl=63 time=82.163 ms
84 bytes from 10.0.0.1 icmp_seq=5 ttl=63 time=38.325 ms

PC1> ping google.com
google.com resolved to 74.125.200.138
84 bytes from 74.125.200.138 icmp_seq=1 ttl=42 time=154.168 ms
84 bytes from 74.125.200.138 icmp_seq=2 ttl=42 time=108.734 ms
84 bytes from 74.125.200.138 icmp_seq=3 ttl=42 time=106.206 ms
84 bytes from 74.125.200.138 icmp_seq=4 ttl=42 time=97.938 ms
84 bytes from 74.125.200.138 icmp_seq=5 ttl=42 time=122.527 ms

PC1> ping 192.168.108.1
192.168.108.1 icmp_seq=1 timeout
192.168.108.1 icmp_seq=2 timeout
192.168.108.1 icmp_seq=3 timeout
192.168.108.1 icmp_seq=4 timeout
192.168.108.1 icmp_seq=5 timeout
```

Sekenario 2:

Disable Rule Drop ICMP

[admin@Nama-Kalian] > ip firewall filter disable numbers=3

[admin@Nama-Kalian] > ip firewall filter add chain=input action=add-src-to-address-list protocol=icmp in-interface=
ether2 address-list=sopoikisingping

[admin@Nama-Kalian] > ip firewall filter add chain=forward action=drop src-address-list=sopoikisingping

Pengujian:

```
PC1> ip dhcp
DORA IP 192.168.108.254/24 GW 192.168.108.1

PC1> ping 192.168.108.1
84 bytes from 192.168.108.1 icmp_seq=1 ttl=64 time=11.236 ms
84 bytes from 192.168.108.1 icmp_seq=2 ttl=64 time=8.394 ms
84 bytes from 192.168.108.1 icmp_seq=3 ttl=64 time=13.013 ms
84 bytes from 192.168.108.1 icmp_seq=4 ttl=64 time=7.056 ms
84 bytes from 192.168.108.1 icmp_seq=5 ttl=64 time=8.891 ms

PC1> ping www.google.com
Cannot resolve www.google.com

PC1> ping google.com
Cannot resolve google.com

PC1>
```

```
PC2> ip dhcp
DORA IP 192.168.108.253/24 GW 192.168.108.1

PC2> ping www.google.com
www.google.com resolved to 10.0.0.1
84 bytes from 10.0.0.1 icmp_seq=1 ttl=63 time=27.877 ms
84 bytes from 10.0.0.1 icmp_seq=2 ttl=63 time=24.932 ms
84 bytes from 10.0.0.1 icmp_seq=3 ttl=63 time=29.979 ms
84 bytes from 10.0.0.1 icmp_seq=4 ttl=63 time=36.341 ms
84 bytes from 10.0.0.1 icmp_seq=5 ttl=63 time=64.641 ms

PC2> ping facebook.com
facebook.com resolved to 31.13.78.35
84 bytes from 31.13.78.35 icmp_seq=1 ttl=82 time=94.086 ms
84 bytes from 31.13.78.35 icmp_seq=2 ttl=82 time=101.724 ms
84 bytes from 31.13.78.35 icmp_seq=3 ttl=82 time=117.943 ms
84 bytes from 31.13.78.35 icmp_seq=4 ttl=82 time=104.530 ms
84 bytes from 31.13.78.35 icmp_seq=5 ttl=82 time=94.307 ms
```

```
[admin@Nama-Kalian] > ip firewall address-list pr
Flags: X - disabled, D - dynamic
 #    LIST                                            ADDRESS                         TIMEOUT
 0 D sopoikisingping                                  192.168.108.254
[admin@Nama-Kalian] >
```

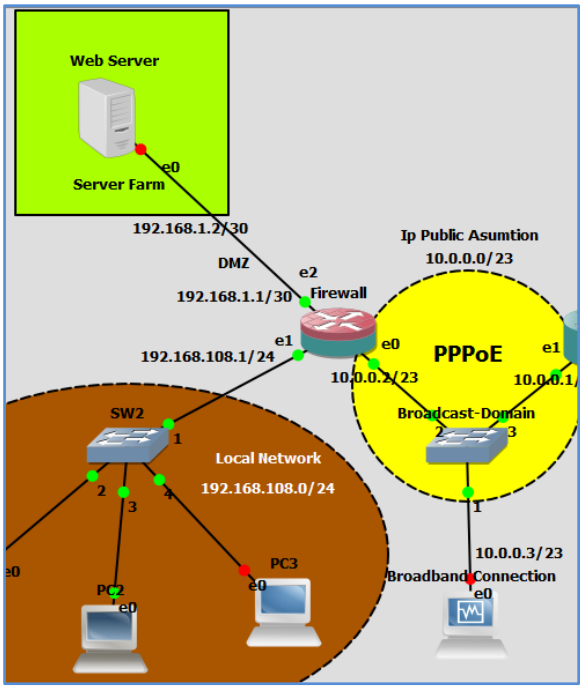
- Penjelasan

  Pada modul inilah baru anda bisa merasakan mengkonfigurasi keamanan jaringan, setelah modul ini nanti akan dibahasa dst-nat yang bisa disebut juga dengan DMZ(demilitarized zone). Jadi modul sebelumnya masih tahapan persiapan dan mendesain saja, termasuk juga konfigurasi PPPoE, adalah langkah untuk dapat mengkonfigurasi keamanan jaringan.

Modul IV

DST-NAT

- Topologi



- Config

Config Server Farm

Untuk konfigurasi server sama persis dengan mengkonfigurasi web server(Asumsi:Sudah terinstall apache2), kurang lebih langkah-langkahnya sebagai berikut:

```
smkti@ubuntu-server:~$ cd /etc/apache2/sites-available/
smkti@ubuntu-server:/etc/apache2/sites-available$ cp 000-default.conf saiful.id.conf
smkti@ubuntu-server:/etc/apache2/sites-available$ sudo nano saiful.id.conf
```

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com
        ServerName smkti.sch.id
        ServerAlias www.smkti.sch.id
        ServerAdmin webmaster@smkti.sch.id
        DocumentRoot /var/www/saiful.id/public_html/

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog /var/www/saiful.id/logs/error.log
        CustomLog /var/www/saiful.id/logs/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

```
smkti@ubuntu-server:~$ sudo mkdir -p /var/www/saiful.id/public html/
smkti@ubuntu-server:~$ sudo touch /var/www/saiful.id/public_html/index.html
smkti@ubuntu-server:~$ sudo nano /var/www/saiful.id/public_html/index.html
<html>
<head><title>Selamat datang di website saiful.id</title>
</head>
<body>
 <h1>Virtual Hosting anda telah berjalan.Ok deh..
     Trims udah running</h1>
```

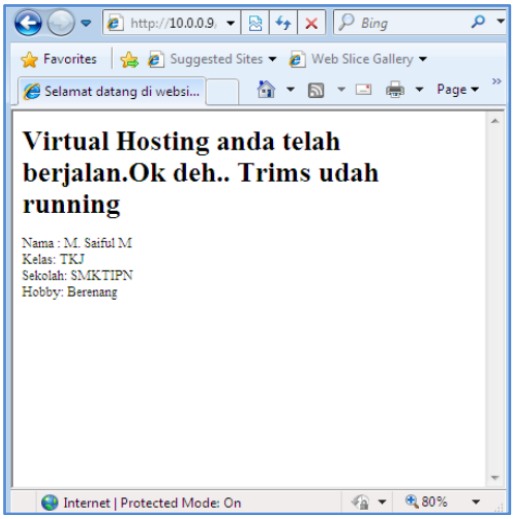
```
 <p>
    Nama : M. Saiful M<br>
    Kelas: TKJ<br>
    Sekolah: SMKTIPN<br>
    Hobby: Berenang
 </p>
</body>
</html>
smkti@ubuntu-server:~$ chown -rf smkti:smkti /var/www/saiful.id/
smkti@ubuntu-server:~$ a2ensite saiful.id.conf
smkti@ubuntu-server:~$ a2dissite 000-default.conf
smkti@ubuntu-server:~$ sudo service apache2 restart
```

```
smkti@ubuntu-server:~$ ls /etc/apache2/sites-enabled/
saiful.id.conf
smkti@ubuntu-server:~$
```

Config Firewall NAT

```
[admin@Nama-Kalian] > ip firewall nat add chain=dstnat action=dst-nat to-
addresses=192.168.1.2 to-ports=80 in-interface=pppoe-out2 dst-port=80 protocol=tcp
```

Pengujian:

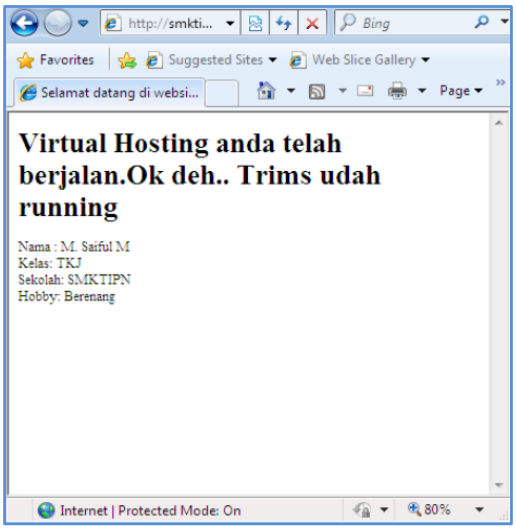


Config ISP DNS Static

[admin@ISP] > ip dns static add name=smktipn.sch.id address=10.0.0.9

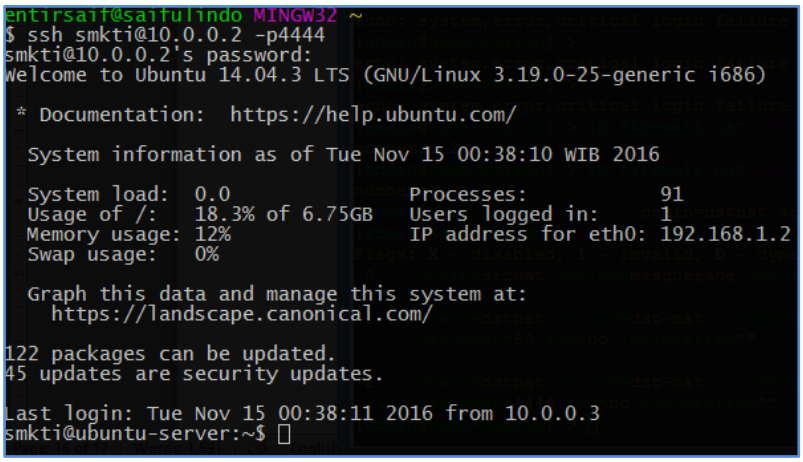
```
[admin@ISP] > ip dns static pr
Flags: D - dynamic, X - disabled, R - regexp
 #     NAME                    ADDRESS                                 TTL
 0     www.google.com          10.0.0.1                                1d
 1     smktipn.sch.id          10.0.0.9                                1d
[admin@ISP] >
```

Pengujian:



- Penjelasan

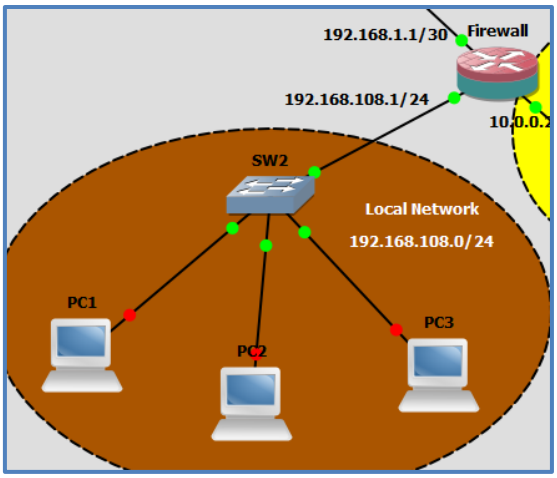
DST-NAT ini intinya adalah bagimana mengijinkan orang lain mengakses ip local(private) menggunakan ip public, jadi memungkinkan mengakses ip private menggunakan akses internet(ip public). Ini berlaku juga pada service-service yang lain seperti ssh, ftp, telnet dan semisalnya. Silahkan anda bereksplorasi dengan service-service yang lain.
Saya telah mencobanya dan berhasil:



Modul IV

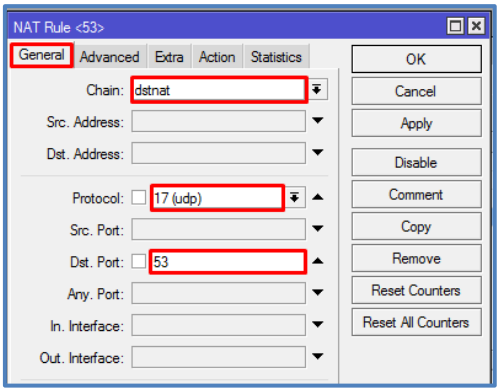
TRANSPARENT DNS

- Topologi

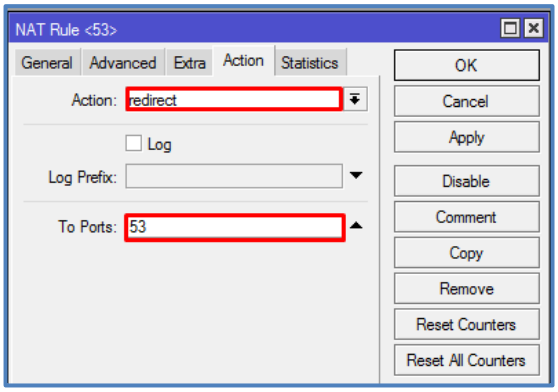


- Config

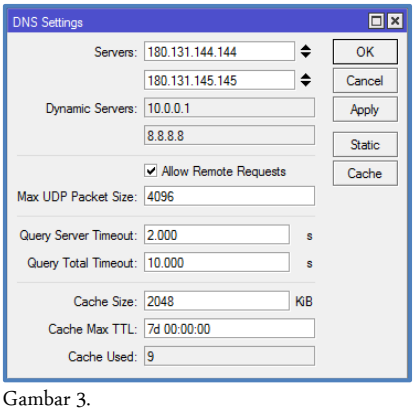
IP > Firewall > NAT



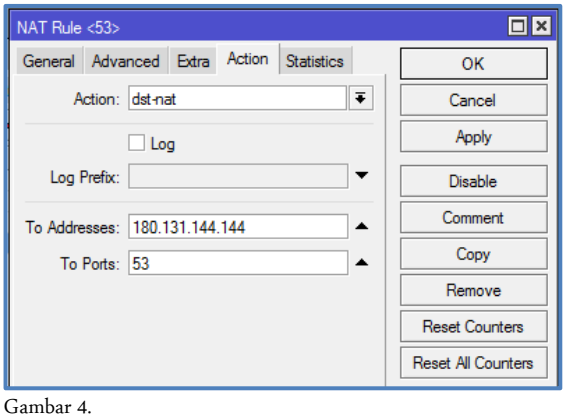
Gambar 1.



Gambar 2.



Gambar 3.



Gambar 4.

```
PC1> ping facebook.com
facebook.com resolved to 31.13.78.35
84 bytes from 31.13.78.35 icmp_seq=1 ttl=82 time=159.388 ms
84 bytes from 31.13.78.35 icmp_seq=2 ttl=82 time=238.965 ms
84 bytes from 31.13.78.35 icmp_seq=3 ttl=82 time=226.854 ms
84 bytes from 31.13.78.35 icmp_seq=4 ttl=82 time=94.087 ms
84 bytes from 31.13.78.35 icmp_seq=5 ttl=82 time=106.145 ms

PC1>
```

```
PC1> ping playboy.com
playboy.com ->> internet-positif.org
internet-positif.org resolved to 118.97.116.27
84 bytes from 118.97.116.27 icmp_seq=1 ttl=53 time=69.378 ms
84 bytes from 118.97.116.27 icmp_seq=2 ttl=53 time=63.814 ms
84 bytes from 118.97.116.27 icmp_seq=3 ttl=53 time=82.947 ms
84 bytes from 118.97.116.27 icmp_seq=4 ttl=53 time=302.874 ms
84 bytes from 118.97.116.27 icmp_seq=5 ttl=53 time=134.182 ms

PC1>
```

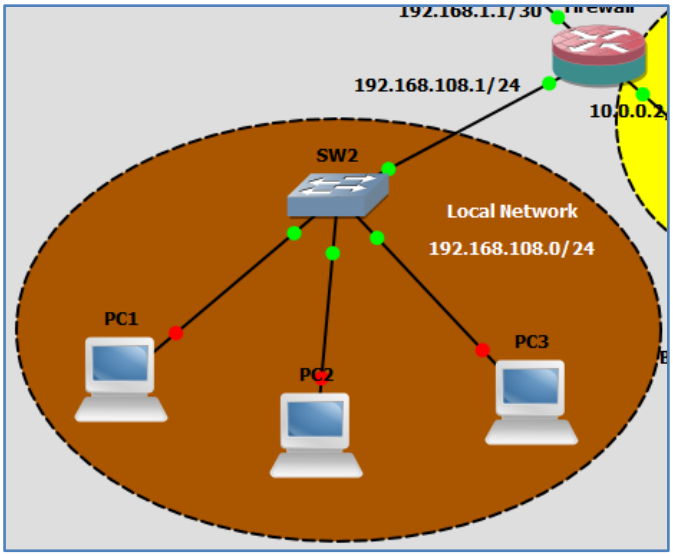
- Penjelasan

Intinya dari Tranparent DNS ini adalah memaksa user menggunakan dns yang di gunakan oleh firewall atau pada Gambar 4. Adalah juga memaksa user menggunakan dns nawala (180.131.144.144) , meskipun user mengganti dnsnya menggunakan dns lain. Ini tujuannya adalah ketika di implementasikan untuk internet sehat. Nawala adalah solusi DNS yang digunakan untuk internet sehat.

Modul IV

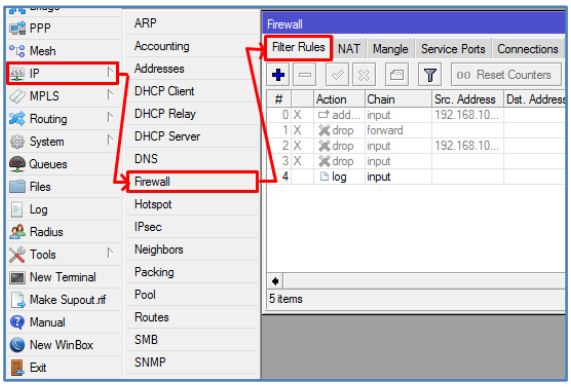
Firewall Logging

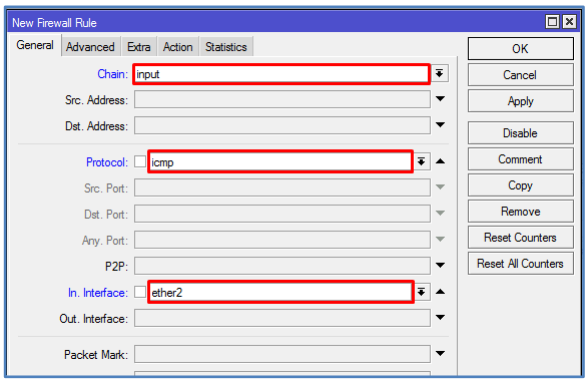
- Topologi

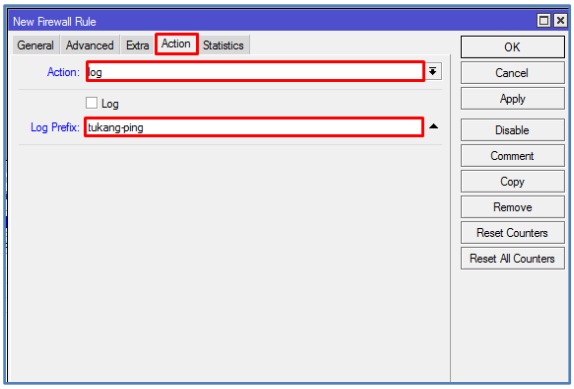


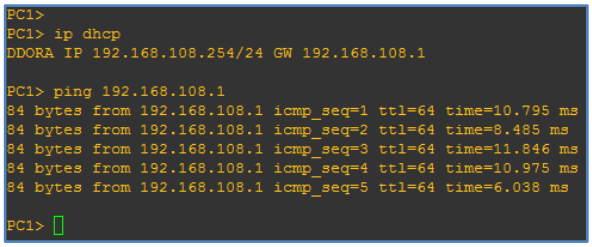
- Config

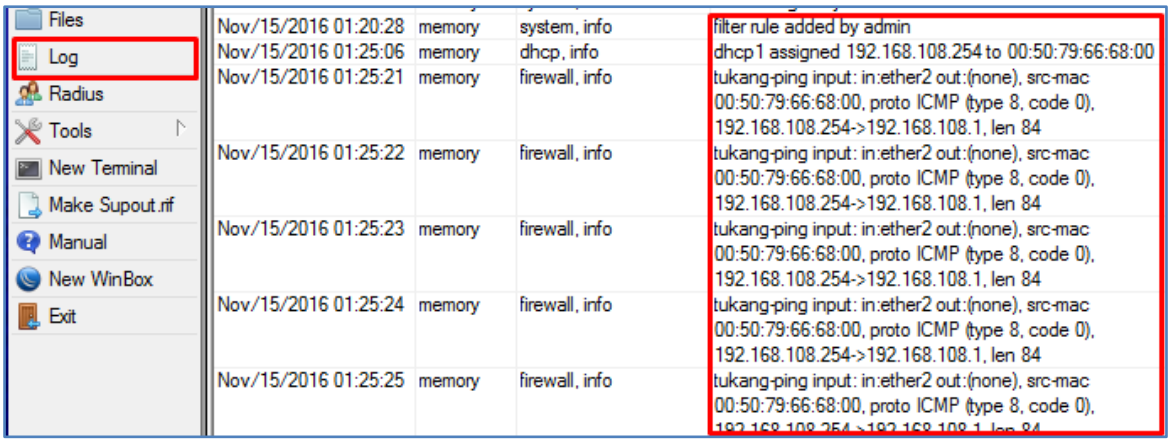
Firewall











Ini menunjukkan bahwa ada host yang melakukan akses protocol icmp menggunakan IP 192.168.108.254 menuju ip 192.168.108.1.

- Penjelasan

  Config diatas adalah melakukan log(pemantauan) ketika ada host dari local network melakukan ping ke firewall, ini merupakan alert bagi administrator, untuk melakukan tindakan persuasif.

Penutup

Selesai sudah modul ini di susun, semoga dapat bermanfaat bagi pembaca sekalian semua, jika ada kesalahan penulisan jangan sungkan-sungkan untuk menghubungi kami di alamat email ritnesaif@gmail.com atau via twitter di @saifulindo.

Dan jikalau ada konfigurasi yang lebih simple bisa di infokan ke kita untuk kita perbaiki file sourcenya, sehingga diharapkan dapat diambil manfaatnya lebih banyak.

Motto: "*Pentingnya proses pembelajaran*" kalimat ini bisa dimaknai "*mengerti sebelum diberitahu*" makanya ada istilah bahasa ibu, bahasa bapak, bahasa guru dan seterusnya.