

**Integrasi Inherent dan Internet menggunakan Routing  
OSPF, NAT, Port Forwarding, Load Balancing, Webproxy  
dengan satu mesin Vyatta**

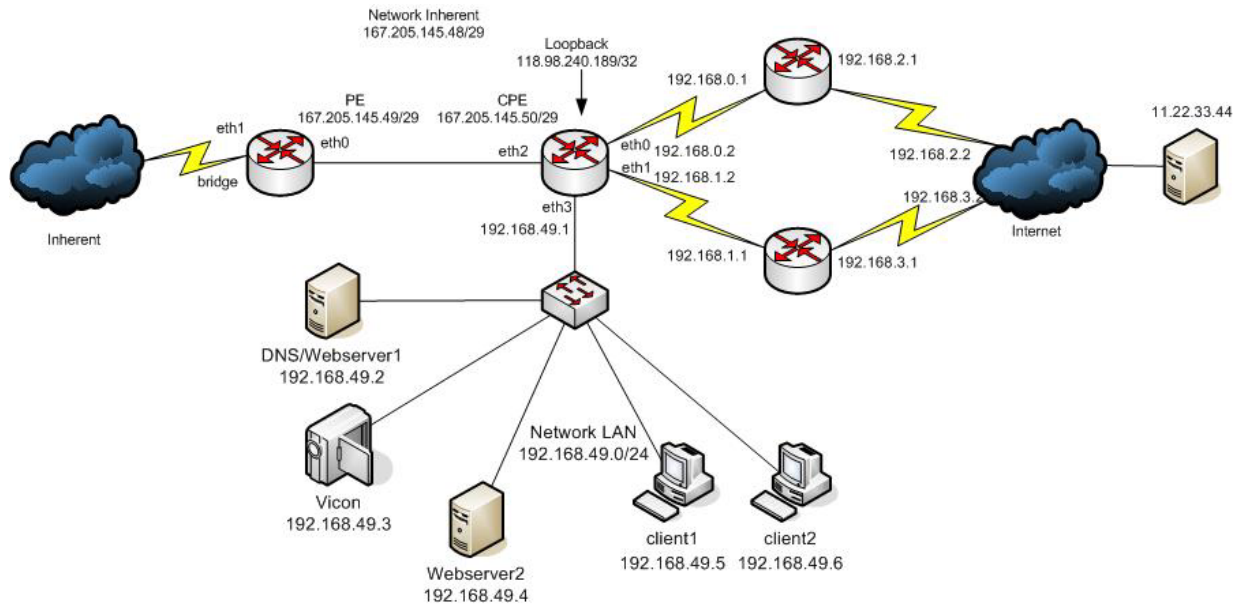
**(Case Study Univ Muhammadiyah Palembang)**

**Candra Setiawan**

**Fakultas Ilmu Komputer**

**Universitas Sriwijaya**

# Topologi



login as: vyatta

vyatta@167.205.145.50's password:

Linux vyatta 2.6.26-1-486-vyatta #1 SMP Fri Feb 27 01:04:20 GMT 2009 i686

Welcome to Vyatta.

This system is open-source software. The exact distribution terms for each module comprising the full system are described in the individual files in /usr/share/doc/\*/copyright.

Last login: Fri Nov 20 01:06:43 2009

Masuk ke configuration mode

```
vyatta@vyatta:~$ configure
```

```
[edit]
```

Set IP address untuk tiap-tiap interfaces

```
vyatta@vyatta# set interfaces ethernet eth0 address 192.168.0.2/24
```

[edit]

```
vyatta@vyatta# set interfaces ethernet eth1 address 192.168.1.2/24
```

[edit]

```
vyatta@vyatta# set interfaces ethernet eth2 address 167.205.145.50/29
```

[edit]

```
vyatta@vyatta# set interfaces ethernet eth2 address 167.205.145.51/29
```

[edit]

```
vyatta@vyatta# set interfaces ethernet eth2 address 167.205.145.52/29
```

[edit]

```
vyatta@vyatta# set interfaces ethernet eth3 address 192.168.49.1/24
```

[edit]

Set Routing Protocol OSPF, disini kita akan mengatur alamat network yang menggunakan OSPF yaitu alamat network 167.205.145.48/29 dan alamat network 118.98.240.189/32 dan ingat jangan pernah meng-advertise alamat IP Private ke Network Inherent.

```
vyatta@vyatta# set protocols ospf log-adjacency-changes
```

[edit]

```
vyatta@vyatta# set protocols ospf parameters router-id 118.98.240.189
```

[edit]

```
vyatta@vyatta# set protocols ospf parameters router-id 118.98.240.189
```

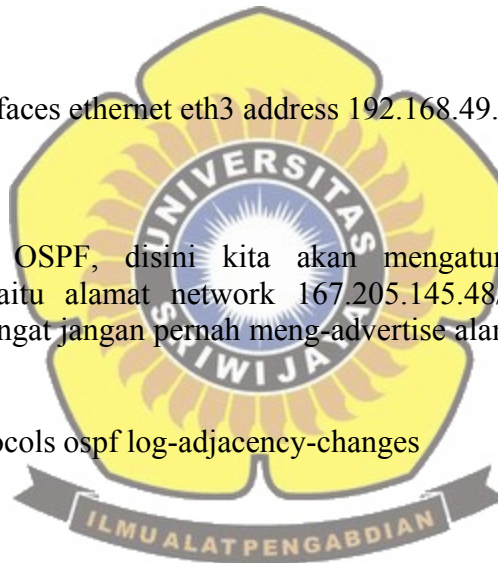
[edit]

```
vyatta@vyatta# set protocols ospf area 69 network 167.205.145.48/29
```

[edit]

```
vyatta@vyatta# set protocols ospf area 69 network 118.98.240.189/32
```

[edit]



Aktifkan webgui untuk vyatta sehingga kita bisa melakukan administrasi mesin vyatta tidak hanya melalui console tetapi juga melalui web. Anda bisa membuka <https://alamat-ip-dari-mesin-vyatta> misal <https://167.205.145.50>

```
vyatta@vyatta# set service https
```

```
[edit]
```

```
vyatta@vyatta# commit
```

```
Generating a 1024 bit RSA private key
```

```
....++++++
```

```
.....++++++
```

```
writing new private key to '/etc/lighttpd/server.pem'
```

```
—
```

```
Stopping web server: lighttpd.
```

```
Starting web server: lighttpd.
```

```
Stopping PAGER server
```

```
saveStarting PAGER server
```

```
[edit]
```

```
vyatta@vyatta# save
```

```
Saving configuration to '/opt/vyatta/etc/config/config.boot'...
```

```
Done
```

```
[edit]
```

```
Set NAT menuju ke inherent
```

```
vyatta@vyatta# set service nat rule 10 description NAT-to-Inherent
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 10 outbound-interface eth2
```



[edit]

```
vyatta@vyatta# set service nat rule 10 type masquerade
```

[edit]

```
vyatta@vyatta# commit
```

[edit]

```
vyatta@vyatta# save
```

Saving configuration to '/opt/vyatta/etc/config/config.boot'...

Done

[edit]

Sampai sini kita sudah bisa mengakses Inherent tetapi berada dalam kondisi NAT

Sekarang bagaimana jika kita ingin agar server kita juga bisa diakses dari inherent dengan mempergunakan IP address yang dialokasikan oleh pengelola inherent sesuai dengan IP address untuk local node kita, padahal server kita ke mempunyai IP Private, disini kita akan memperlakukan satu teknik lagi, yang dikenal dengan IP Forwarding jika kita ingin meneruskan seluruh traffic dari inherent ke server kita, dan Port Forwarding jika kita ingin meneruskan traffic ke port tertentu saja misal vyatta hanya akan meneruskan ke mesin local jika ada request menuju ke port 80 (http). Disini kita akan memperlakukan teknik Port Forwarding. Contoh disini kita menginginkan agar alamat IP server local 192.168.49.2 bisa diakses dari inherent dengan IP address 167.205.145.51 dengan protocol http (Port 80).

```
vyatta@vyatta# set service nat rule 20 description DNAT-to-Webserver1-from-inherent
```

[edit]

```
vyatta@vyatta# set service nat rule 20 type destination
```

[edit]

```
vyatta@vyatta# set service nat rule 20 destination address 167.205.145.51
```

[edit]

```
vyatta@vyatta# set service nat rule 20 inbound-interface eth2
```

[edit]

```
vyatta@vyatta# set service nat rule 20 protocol tcp
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 20 destination port 80
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 20 inside-address address 192.168.49.2
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 20 inside-address port 80
```

```
[edit]
```

```
vyatta@vyatta# commit
```

```
[edit]
```

```
vyatta@vyatta# save
```

```
Saving configuration to '/opt/vyatta/etc/config/config.boot'...
```

```
Done
```

```
[edit]
```

Nah sekarang bagaimana jika kita mempunyai alat Vicon untuk melakukan telekonferensi, Komunikasi voice dan video ini mempergunakan protocol UDP sebagai protocol transport-nya, nah disini kita akan melakukan IP Forwarding, artinya meneruskan seluruh traffic tanpa perlu memperhatikan traffic tersebut mempergunakan protocol transport apa dan nomor port berapa sebagai destination port-nya.

```
vyatta@vyatta# set service nat rule 30 description DNAT-to-Vicon-from-inherent
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 30 type destination
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 30 destination address 167.205.145.52
```

```
[edit]
```



```
vyatta@vyatta# set service nat rule 30 inbound-interface eth2
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 30 inside-address address 192.168.49.3
```

```
[edit]
```

```
vyatta@vyatta#
```

Nah pada saat anda memberikan IP pada vicon berikanlah IP Private 192.168.49.3, dan sampai disini berarti baik webserver dan vicon kita sudah bisa berkomunikasi 2 arah dalam artian bisa mengakses dan bisa diakses dari jaringan inherent

Selanjutnya bagaimana kita bisa memanfaatkan IP public pada modem ADSL kita untuk bisa diberikan ke webserver kita, sebenarnya teknik yang dipergunakan sama seperti sebelumnya yaitu teknik Port Forwarding. Pada permodelan network ini kita anggap IP Address 192.168.0.2 dan IP Address 192.168.1.2 adalah IP Public

```
vyatta@vyatta# set service nat rule 40 description DNAT-from-ISP1-to-webserver1
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 40 type destination
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 40 destination address 192.168.0.2
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 40 protocol tcp
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 40 destination port 80
```

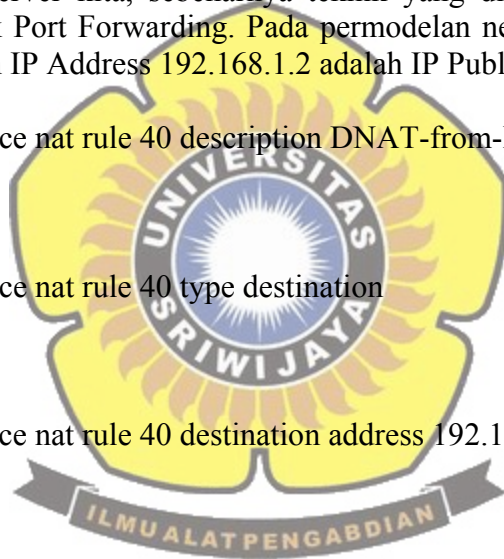
```
[edit]
```

```
vyatta@vyatta# set service nat rule 40 inbound-interface eth0
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 40 inside-address address 192.168.49.2
```

```
[edit]
```



```
vyatta@vyatta# set service nat rule 40 inside-address port 80
```

```
[edit]
```

Nah sekarang server tersebut juga sudah bisa di akses dari internet dengan mempergunakan IP Public, lakukan pendaftaran ke <http://pandi.or.id> agar server tersebut bisa diakses dengan mempergunakan nama domain

Sekarang kita akan memanfaatkan IP Public satu yaitu lagi 192.168.1.2 untuk diberikan ke server kita yang lain, bisa jadi server ini akan kita jadikan mail server ataupun server yang lain sesuai dengan kebutuhan kita. Dan ingat jika anda ingin menjadikan server ini sebagai mail server, mau tidak mau yang harus anda lakukan adalah melakukan pendaftaran domain ke <http://pandi.or.id> karena mail server harus mempunyai MX record sehingga MTA dari mail server lain bisa mengirim email ke server kita (komunikasi antar mail server). Tetapi untuk contoh disini kita masih mempergunakan port 80 karena kita ingin agar server kita ini juga berfungsi penyedia layanan web dan bisa dimanfaatkan untuk layanan e-learning dan lain-lain.

```
vyatta@vyatta# set service nat rule 50 description DNAT-from-ISP2-to-webserver2
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 50 type destination
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 50 destination address 192.168.1.2
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 50 protocol tcp
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 50 destination port 80
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 50 inbound-interface eth0
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 50 inside-address address 192.168.49.4
```

```
[edit]
```





```
vyatta@vyatta# set service nat rule 50 inside-address port 80
```

```
[edit]
```

```
vyatta@vyatta# commit
```

```
[edit]
```

```
vyatta@vyatta# save
```

```
Saving configuration to '/opt/vyatta/etc/config/config.boot' ...
```

```
Done
```

```
[edit]
```

Kemudian lakukan NAT menuju ke internet melalui ISP1 supaya user pada LAN bisa mengakses layanan internet

```
vyatta@vyatta# set service nat rule 60 description NAT-to-Internet-via-ISP1
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 60 destination address 0.0.0.0/0
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 60 outbound-interface eth0
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 60 type masquerade
```

```
[edit]
```

```
vyatta@vyatta# commit
```

```
[edit]
```

```
vyatta@vyatta# save
```

```
Saving configuration to '/opt/vyatta/etc/config/config.boot' ...
```

```
Done
```

```
[edit]
```



Sama seperti diatas lakukan NAT sekali lagi menuju ke internet melalui ISP2

```
vyatta@vyatta# set service nat rule 70 description NAT-to-Internet-via-ISP2
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 70 destination address 0.0.0.0/0
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 70 outbound-interface eth1
```

```
[edit]
```

```
vyatta@vyatta# set service nat rule 70 type masquerade
```

```
[edit]
```

```
vyatta@vyatta# commit
```

```
[edit]
```

```
vyatta@vyatta# save
```

```
Saving configuration to '/opt/vyatta/etc/config/config.boot'...
```

```
Done
```

```
[edit]
```

Set default gateway baik yang melalui ISP1 dan ISP2

```
vyatta@vyatta# set protocols static route 0.0.0.0/0 next-hop 192.168.0.1
```

```
[edit]
```

```
vyatta@vyatta# set protocols static route 0.0.0.0/0 next-hop 192.168.1.1
```

```
[edit]
```

Sekarang kita akan mencoba melihat routing table yang terbentuk

```
vyatta@vyatta#exit
```

```
[edit]
```



```
vyatta@vyatta:~$ show ip route
```

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,

I - ISIS, B - BGP, > - selected route, \* - FIB route

```
S>* 0.0.0.0/0 [1/0] via 192.168.0.1, eth0
```

```
* via 192.168.1.1, eth1
```

```
O 118.98.240.189/32 [110/10] is directly connected, lo, 00:59:56
```

```
C>* 118.98.240.189/32 is directly connected, lo
```

```
C>* 127.0.0.0/8 is directly connected, lo
```

```
O 167.205.145.48/29 [110/10] is directly connected, eth2, 01:15:48
```

```
C>* 167.205.145.48/29 is directly connected, eth2
```

```
C>* 192.168.0.0/24 is directly connected, eth0
```

```
C>* 192.168.1.0/24 is directly connected, eth1
```

```
O>* 192.168.5.0/24 [110/20] via 167.205.145.49, eth2, 01:15:47
```

```
C>* 192.168.49.0/24 is directly connected, eth3
```

```
vyatta@vyatta:~$
```

```
[edit]
```

Note:

Perlu dicatat disini, karena ini merupakan simulasi dengan VMware maka routing table yang terbentuk terbatas pada network-network yang ada pada simulasi ini. Routing Table akan terbentuk lebih banyak lagi jika kita sudah menghubungkan router ini ke real system.

Set load balancing baik melalui eth0 maupun eth1

```
vyatta@vyatta:~$configure
```

```
[edit]
```

```
vyatta@vyatta# set load-balancing wan interface-health eth0 failure-count 5
```



[edit]

```
vyatta@vyatta# set load-balancing wan interface-health eth0 nexthop 192.168.0.1
```

[edit]

```
vyatta@vyatta# set load-balancing wan interface-health eth0 ping 192.168.0.1
```

[edit]

```
vyatta@vyatta# set load-balancing wan interface-health eth1 failure-count 4
```

[edit]

```
vyatta@vyatta# set load-balancing wan interface-health eth1 nexthop 192.168.1.1
```

[edit]

```
vyatta@vyatta# set load-balancing wan interface-health eth1 ping 192.168.1.1
```

[edit]

Set rule (pengaturan) dari load balancing agar traffic yang berasal eth3 (LAN) bisa diarahkan keluar melalui eth0 dan eth1, berikan rule 10

```
vyatta@vyatta# set load-balancing wan rule 10 inbound-interface eth3
```

[edit]

```
vyatta@vyatta# set load-balancing wan rule 10 interface eth0 weight 2
```

[edit]

```
vyatta@vyatta# set load-balancing wan rule 10 interface eth1 weight 1
```

[edit]

```
vyatta@vyatta# commit
```

[edit]

```
vyatta@vyatta# save
```

Saving configuration to '/opt/vyatta/etc/config/config.boot'...

Done



[edit]

vyatta@vyatta#

Set lagi rule (pengaturan) dari load balancing seperti diatas, kali ini berikan rule 20

vyatta@vyatta# set load-balancing wan rule 20 inbound-interface eth3

[edit]

vyatta@vyatta# set load-balancing wan rule 20 interface eth0 weight 2

[edit]

vyatta@vyatta# set load-balancing wan rule 20 interface eth1 weight 1

[edit]

vyatta@vyatta# commit

[edit]

vyatta@vyatta# save

Saving configuration to '/opt/vyatta/etc/config/config.boot'...

Done

[edit]

Jika anda menjadikan server pada alamat IP 192.168.49.2 sebagai DNS local maka pada mesin vyatta arahkan name server menuju IP tersebut

vyatta@vyatta# set system name-server 192.168.49.2

[edit]

Untuk menghemat penggunaan bandwidth maka Vyatta juga bisa dijadikan webproxy yang bisa menyimpan web cache, dan karena seluruh traffic dari LAN akan menuju alamat IP 192.168.49.1 maka alamat IP ini berfungsi sebagai default gateway untuk LAN tersebut, atur listen-address untuk menggunakan IP tersebut.

vyatta@vyatta# set service webproxy listen-address 192.168.49.1

[edit]



```
vyatta@vyatta# commit
```

```
Restarting Squid HTTP Proxy 3.0: squid3.
```

```
[edit]
```

```
vyatta@vyatta# save
```

```
Saving configuration to '/opt/vyatta/etc/config/config.boot' ...
```

```
Done
```

```
[edit]
```

```
Lakukan updating terhadap webproxy
```

```
vyatta@vyatta# exit
```

```
exit
```

```
vyatta@vyatta:~$ update webproxy blacklists
```

```
Warning: No url-filtering blacklist installed
```

```
Would you like to download a default blacklist? [confirm][y]
```

```
-2009-11-22 20:51:06- ftp://ftp.univ-  
tlse1.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz
```

```
=> `/tmp/blacklists.gz'
```



---

-cut-

```
Masuk lagi ke configure mode buat pengaturan untuk web proxy ini
```

```
vyatta@vyatta:~$ configure
```

```
[edit]
```

```
Alokasikan besarnya cache webproxy pada hardisk, nilai yang kita buat dalam ukuran MB, contoh angka 100000 berarti 100000 MB. Lakukan sesuai dengan ketersediaan space yang tersedia pada hardisk anda.
```

```
vyatta@vyatta # set service webproxy cache-size 100000
```

```
[edit]
```

Set auto update seminggu sekali supaya tidak terlalu membebani bandwidth

```
vyatta@vyatta # set service webproxy url-filtering squidguard auto-update weekly
```

[edit]

Set alamat url yang tidak kita izinkan untuk diakses, misal link game pada facebook, karena konsumsi bandwidth yang cukup besar

```
vyatta@vyatta # set service webproxy url-filtering squidguard local-block  
apps.facebook.com
```

[edit]

Set kategori yang bersifat pornografi dan perjudian maupun kategori yang dilarang lainnya, tetapi anda harus hati-hati dan cukup bijak terhadap content ini, karena beberapa fakultas seperti fakultas kedokteran memerlukan keyword sex untuk menunjang pembelajaran mereka dalam mencari literatur, jurnal dan lain sebagainya

```
vyatta@vyatta# set service webproxy url-filtering squidguard block-category sex
```

[edit]

Redirect-url berguna untuk membelokkan traffic jika ada user mengakses content yang termasuk dalam kategori yang dilarang tadi, misal dibelokkan menuju ke official site kita: [www.unsri.ac.id](http://www.unsri.ac.id)

```
vyatta@vyatta # set service webproxy url-filtering squidguard redirect-url  
www.unsri.ac.id
```

[edit]

```
vyatta@vyatta # commit
```

[edit]

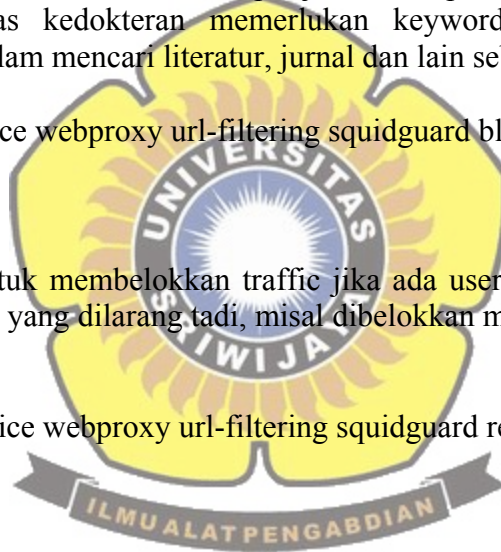
```
vyatta@vyatta # save
```

Saving configuration to '/opt/vyatta/etc/config/config.boot' ...

Done

[edit]

```
vyatta@vyatta #
```



Demikianlah desain dari network ini kami (Tim ICT Unsri) buat sebagai bentuk kepedulian kami terhadap kemajuan bersama berdasarkan asas Tri Dharma Perguruan Tinggi. Bagaimana kita membuat suatu system yang handal berdasarkan kondisi existing dari network tersebut dan tetap memperhatikan aspek *low cost, low requirement and still meet with user requirement but powerful* dengan memanfaatkan Vyatta Open Source (Thanks to Vyatta <http://vyatta.org>) dan *low end PC* (PC Butut). Terhadap Universitas lain yang berada di bawah sub local node Palembang-UNSRI, kami sangat terbuka untuk saling membantu dalam perancangan network, berdiskusi, dan saling berbagi. *Let share and discuss guy..remember IT not cost centre*

