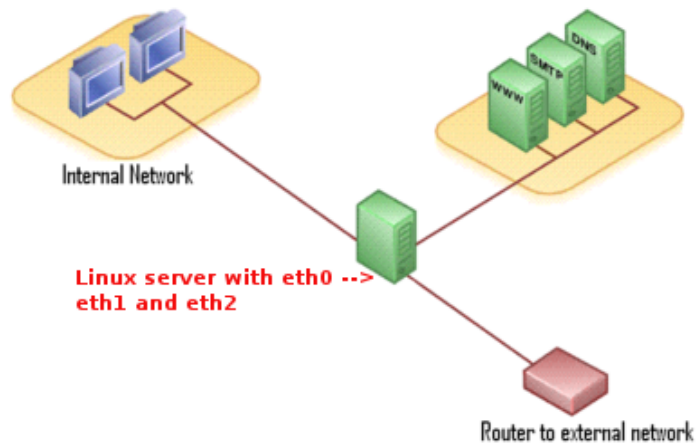
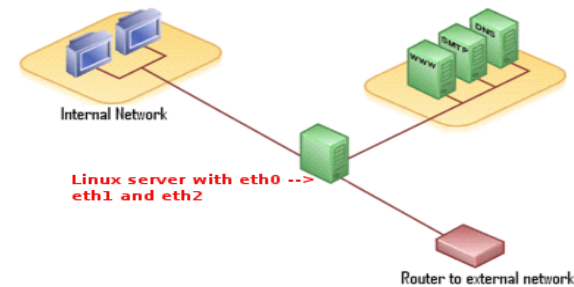


Iptables - DMZ



- eth0 with 192.168.1.1 private IP address - Internal LAN ~ Desktop system
- eth1 with 202.54.1.1 public IP address - WAN connected to ISP router
- eth2 with 192.168.2.1 private IP address - DMZ connected to Mail / Web / DNS and other private servers

Routing traffic between public and DMZ server



- To set a rule for routing all incoming SMTP requests to a dedicated Mail server at IP address 192.168.2.2 and port 25, network address translation (NAT) calls a PREROUTING table to forward the packets to the proper destination.
- This can be done with appropriate IPTABLES firewall rule to route traffic between LAN to DMZ and public interface to DMZ. For example, all incoming mail traffic from internet (202.54.1.1) can be send to DMZ mail server (192.168.2.2) with the following iptables prerouting rule (assuming default DROP all firewall policy):

Routing traffic between public and DMZ server

end init firewall .. Start DMZ stuff

forward traffic between DMZ and LAN

```
iptables -A FORWARD -i eth0 -o eth2 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A FORWARD -i eth2 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

forward traffic between DMZ and WAN servers SMTP, Mail etc

```
iptables -A FORWARD -i eth2 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A FORWARD -i eth1 -o eth2 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

Route incoming SMTP (port 25) traffic to DMZ server 192.168.2.2

```
iptables -t nat -A PREROUTING -p tcp -i eth1 -d 202.54.1.1 --dport 25 -j DNAT --to-destination 192.168.2.2
```

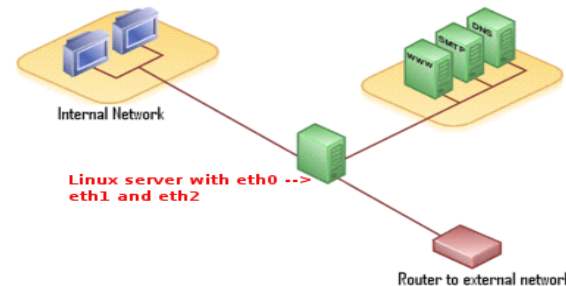
Route incoming HTTP (port 80) traffic to DMZ server load balancer IP 192.168.2.3

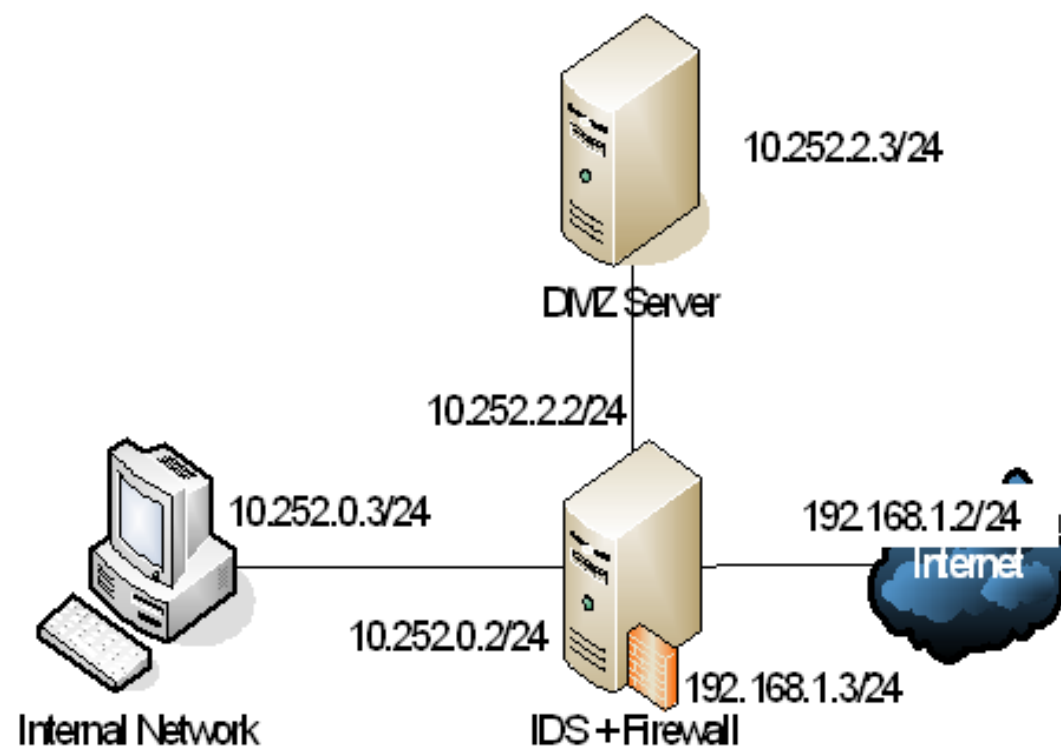
```
iptables -t nat -A PREROUTING -p tcp -i eth1 -d 202.54.1.1 --dport 80 -j DNAT --to-destination 192.168.2.3
```

Route incoming HTTPS (port 443) traffic to DMZ server reverse load balancer IP 192.168.2.4

```
iptables -t nat -A PREROUTING -p tcp -i eth1 -d 202.54.1.1 --dport 443 -j DNAT --to-destination 192.168.2.4
```

End DMZ .. Add other rules





- Bangun Jaringan dan konfigurasi sendiri seperti gambar diatas.
- Install web server, FTP Server, dan Telnet pada jaringan DMZ server
- Untuk instalasi webserver, FTP server dan telnet
- # apt-get install apache2 proftpd telnetd
- - Buat statefull firewall :
 - New state diperbolehkan dari internet ke DMZ
 - New state tidak diperbolehkan dari internet ke IDS+firewall dan internal
 - New state diperbolehkan dari internal ke DMZ dan IDS+Firewall
 - New State tidak diperbolehkan dari DMZ Server ke internal, Firewall dan internet
 - New state tidak diperbolehkan dari firewall ke internal network
 - Buat jaringan 192.168.1.2 bisa akses web, ftp tapi tidak bisa akses telnet
 - Buat jaringan 192.168.1.2 tidak boleh melakukan perintah ping ke DMZ server
 - Buat jaringan internal bisa akses web, ftp dan telnet
 - Ceklah rule firewall yang telah anda buat
- #iptables -nL atau #iptables -t nat -nL