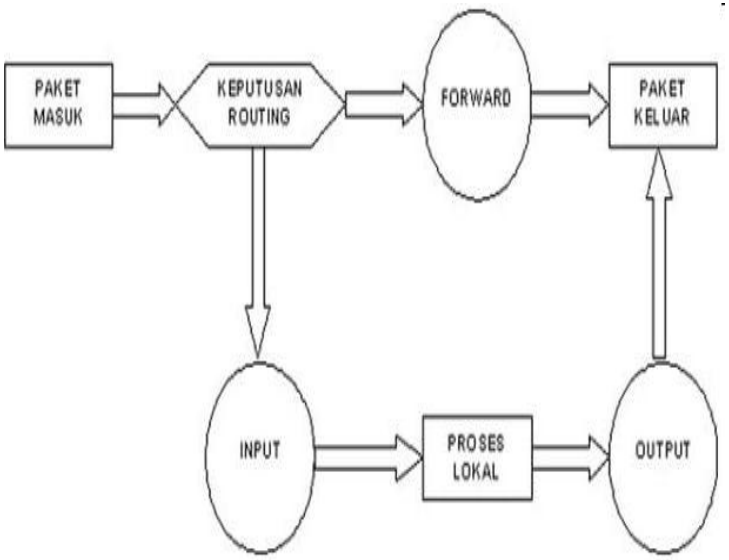
ITS
Institut
Teknologi
Sepuluh Nopember

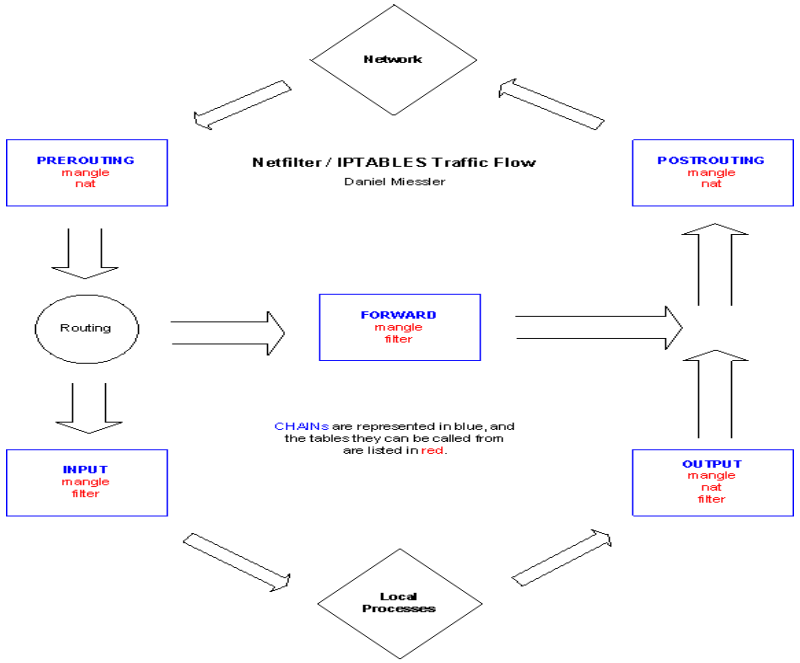
IPTABLES



Prinsip Kerja iptables

- Paket masuk diproses berdasarkan tujuan :
  - Destination IP untuk Firewall → masuk proses input
  - Destination IP bukan untuk firewall tapi diteruskan → masuk proses FORWARD
- Selanjutnya dicocokkan berdasarkan tabel policy yang dipunyai firewall apakah di-accept atau di-drop





Sintaks IPTABLES

- Opsi
  1. -A, menambah satu aturan baru ditempatkan pada posisi terakhir
     iptables –A INPUT …
  1. -D, menghapus rule
     iptables –D INPUT 1
     iptables –D –s 202.154.178.2 …
  2. -I, menambah aturan baru penempatan bisa disisipkan sesuai nomor
     iptables –I INPUT 3 –s 202.154.178.2 –j ACCEPT
  3. -R, mengganti rule
     iptables –R INPUT 2 –s –s 202.154.178.2 –j ACCEPT
  4. -F, menghapus seluruh rule
     iptables –F
  5. -L, melihat Rule
     iptables -L

Parameter

- -p [!] protocol, protokol yang akan dicek
  Iptables –A INPUT –p tcp …
- -s [!] address/[mask], memeriksa kecocokan sumber paket
  Iptables –A INPUT –s 10.252.44.145 …
- -d [!] address/[mask], memerika kecocokan tujuan paket
  Iptables –A INPUT –d 202.154.178.2 …
- -j target, menentukan nasib paket, target misal ACCEPT/DROP/REJECT
  Iptables –A INPUT –d 202.154.178 –j DROP
- -i [!] interface_name, identifikasi kartu jaringan tempat masuknya data
  Iptables –A INPUT –i etho ….
- -o [!] interface_name, identifikasi kartu jaringan tempat keluarnya paket
  Iptables –A OUTPUT –o eth1 ….

Match iptables

- --mac address, matching paket berdasarkan nomor MAC Address

  Iptables –m mac –mac-address 44:45:53:54:00:FF

- Multiport, mendifinisikan banyak port

  Iptables –m multiport –source-port 22,25,110,80 –j ACCEPT

- State, mendefinisikan state dari koneksi

  Iptables –A INPUT –m state –state NEW, ESTABLISH –j ACCEPT

Target/Jump iptables

- ACCEPT, setiap paket langsung diterima

  Iptables –A INPUT –p tcp –dport 80 –j ACCEPT

- DROP, paket datang langsung dibuang

  Iptables –A INPUT –p tcp –dport 21 –j DROP

- REJECT, paket yang ditolak akan dikirimi pesan ICMP error

  Iptables –A INPUT –p tcp –dport 21 –j REJECT

- SNAT, sumber paket dirubah, biasanya yang memiliki koneksi internet

  Iptables –t nat –A POSROUTING –p tcp –o eth0 –j SNAT –to-source 202.154.178.2

- DNAT, merubah tujuan alamat paket. Biasanya jika server alamat Ipnya lokal, supaya internet bisa tetap akses diubah ke publik

  Iptables –t nat –A PREPROUTING –p tcp –d 202.154.178.2 –dport 80 –j DNAT –to-destination 192.168.1.1

- MASQUERADE, untuk berbagi koneksi internet dimana no_ipnya terbatas, sebagai mapping ip lokal ke publik

  Iptables –t nat –A POSTROUTING –o eth0 –dport 80 –j MASQUERADE

- REDIRECT, sigunakan untuk transparent proxy

  Ipatbles –t nat –A PREROUTING –p tcp –d 0/0 –dport 80 –j REDIRECT –to-port 8080

- LOG, melakukan pencatatan terhadap aktifitas firewall kita, untuk melihat bisa dibuka /etc/syslog.conf

  Iptables –A FORWARD –j LOG –log-level-debug

  Iptables –A FORWARD –j LOG –log-tcp-options

Firewall Option

- # Mengeluarkan Modul-modul Iptables
- /sbin/modprobe ip_tables
- /sbin/modprobe ip_conntrack
- /sbin/modprobe iptable_filter
- /sbin/modprobe iptable_mangle
- /sbin/modprobe iptable_nat
- /sbin/modprobe ipt_LOG
- /sbin/modprobe ipt_limit
- /sbin/modprobe ipt_state
- /sbin/modprobe ip_conntrack_ftp
- /sbin/modprobe ip_conntrack_irc
- /sbin/modprobe ip_nat_ftp
- /sbin/modprobe ip_nat_irc

Menghapus Rule iptables

- # Menghapus aturan iptables

```
$IPTABLES -F
$IPTABLES -t nat -F
$IPTABLES -t mangle -F
```

- # Menghapus nama kolom yg dibuat manual

```
$IPTABLES -X
$IPTABLES -t nat -X
$IPTABLES -t mangle -X
```

Modul 5 DoS Rev.doc - Microsoft Word

File Edit View Insert Format Tools Table Window Help Adobe PDF Acroba

isbat@www: ~/public_html/security

```
--- 10.252.44.178 ping statistics ---
94 packets transmitted, 0 received, 100% packet loss, time 9301

www:/home/isbat/public_html/security# ping 10.252.44.178
PING 10.252.44.178 (10.252.44.178) 56(84) bytes of data.
64 bytes from 10.252.44.178: icmp_seq=1 ttl=64 time=0.295 ms
64 bytes from 10.252.44.178: icmp_seq=2 ttl=64 time=0.264 ms
64 bytes from 10.252.44.178: icmp_seq=3 ttl=64 time=0.381 ms
^C
--- 10.252.44.178 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.264/0.313/0.381/0.051 ms
www:/home/isbat/public_html/security# ping 10.252.44.178
PING 10.252.44.178 (10.252.44.178) 56(84) bytes of data.
```

isbat@latihan: ~

```
target     prot opt source               destination
DROP       0    --  localnet/24          anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
latihan:/home/isbat# /sbin/iptables -A INPUT -p icmp -s 10.252.44.
latihan:/home/isbat# iptables -F
latihan:/home/isbat# /sbin/iptables -A INPUT -p icmp -s 10.252.44.
latihan:/home/isbat#
```

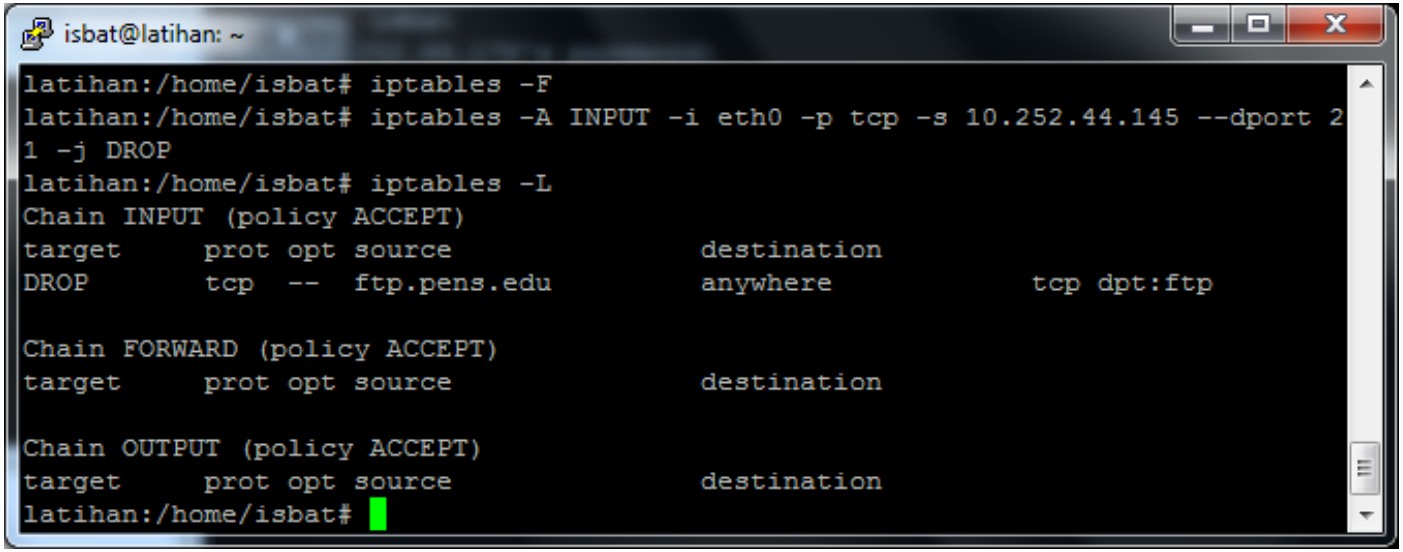
t --limit 5/s -j ACCEPT

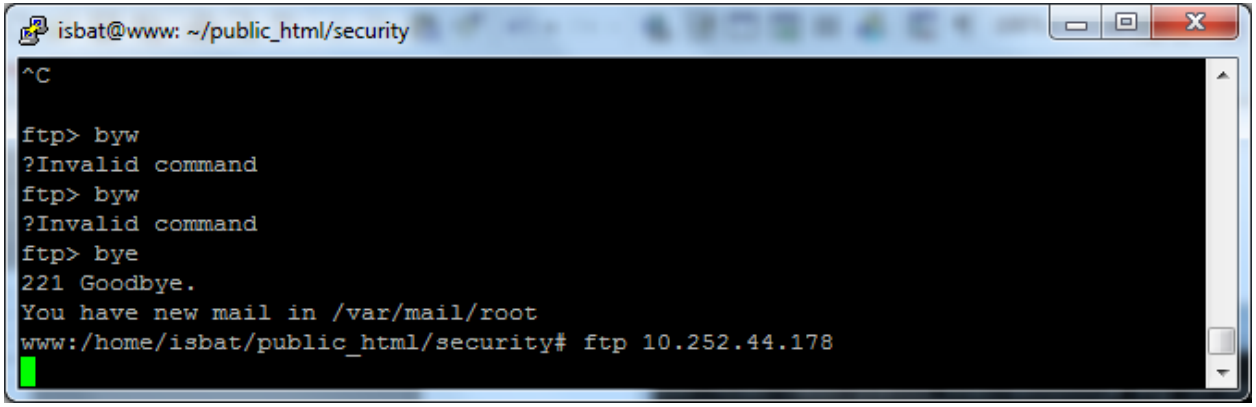
isbat@latihan: ~

```
17:39:04.807486 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 58686, seq 93, length
17:39:05.807553 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 58686, seq 94, length
17:39:17.138940 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 59710, seq 1, length 6
17:39:18.138007 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 59710, seq 2, length 6
17:39:19.137200 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 59710, seq 3, length 6
17:39:22.138900 arp reply ftp.pens.edu is-at 00:00:e2:9a:c3:0e (oui Unknown)
17:39:27.570566 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 1, length 64
17:39:28.585373 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 2, length 64
17:39:29.585440 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 3, length 64
17:39:30.585507 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 4, length 64
17:39:31.585573 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 5, length 64
17:39:32.585641 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 6, length 64
17:39:33.585708 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 7, length 64
17:39:34.585775 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 8, length 64
17:39:35.585842 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 9, length 64
17:39:36.585909 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 10, length 6
17:39:37.585976 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 11, length 6
17:39:38.586044 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 12, length 6
17:39:39.586235 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 13, length 6
17:39:40.586302 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 14, length 6
17:39:41.586369 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 15, length 6
17:39:42.586436 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 16, length 6
```

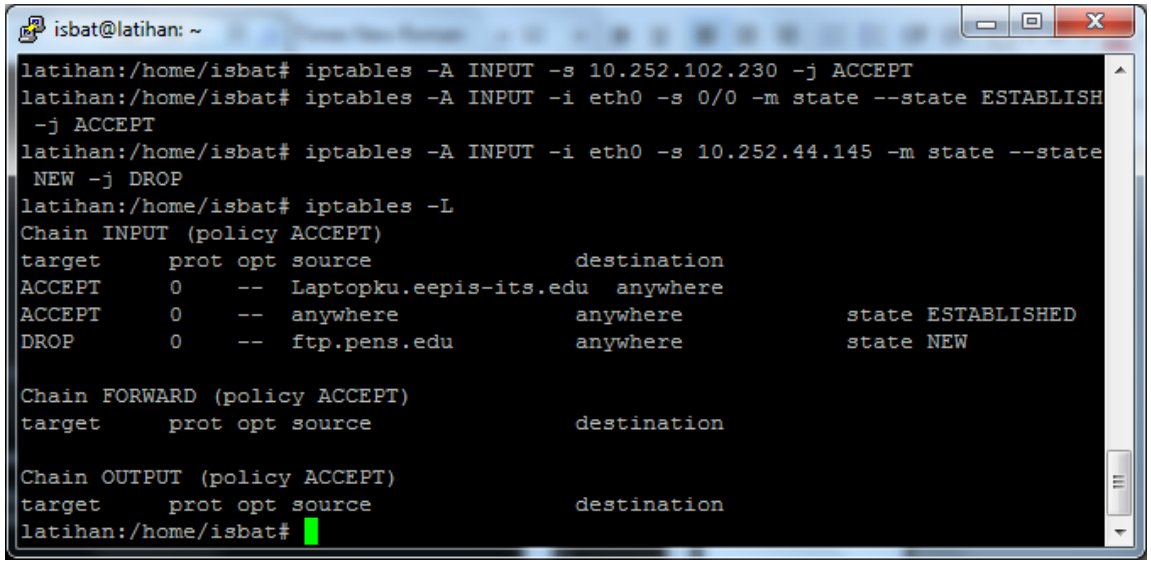
Page 10 Sec 1 10/12 At 9.7" Ln 15 Col 1 REC TRK EXT OVR English (U.S.

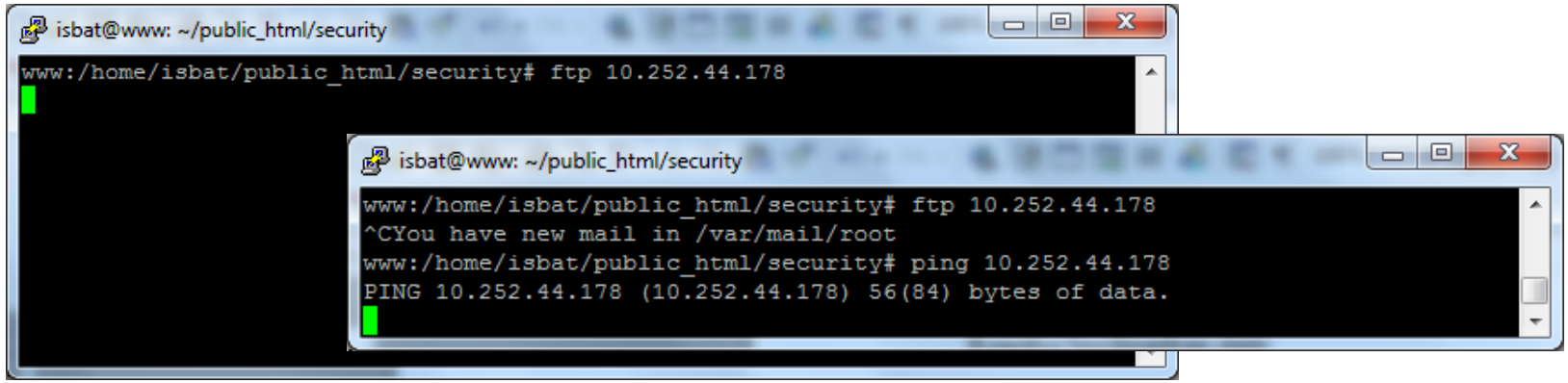
Packet Filtering Firewall



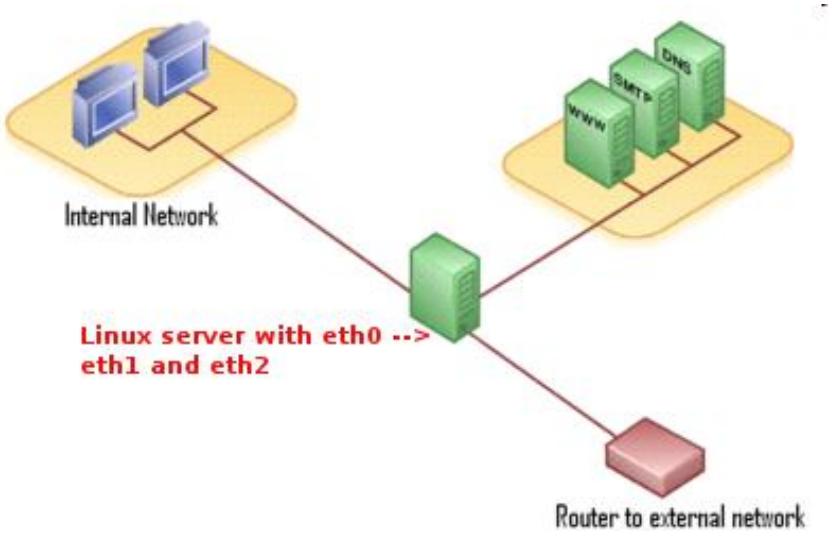


Circuit Level Gateway



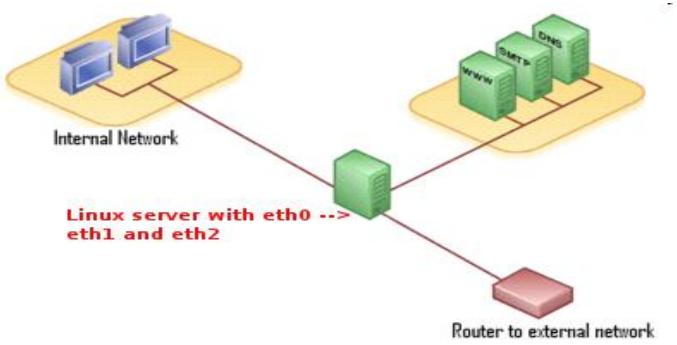


Iptables - DMZ



- 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

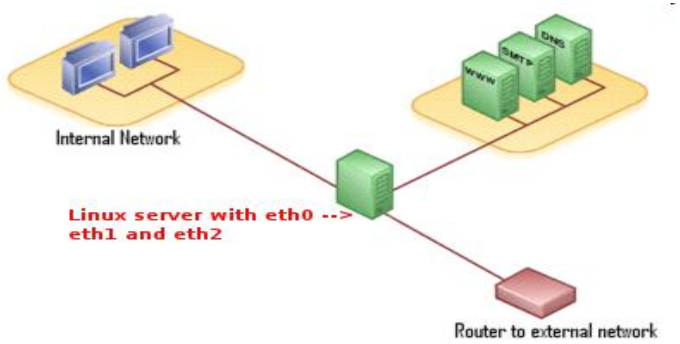
Routing traffic between public and DMZ server



- 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 ###
```