# 1) Set the default INPUT and FORWARD policy to DROP

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
```

# 2) Allow communications between LAN and DMZ machines

```
iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

# Allow LAN machines to initiate communication to INT, and receive responses

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

# Allow DMZ machines to initiate communication to INT, and receive responses

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

# 3) For communication initiated from INT to DMZ machines, allow connection only to port 22 on the SSH machine and to port 80 on HTTP machine; subsequently, responses should be allowed to go back to INT

```
iptables -A FORWARD -i eth2 -o eth1 -p tcp --dport 22 -d 123.123.1.100/24 -j ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -p tcp --dport 80 -d 123.123.1.100/24 -j ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

# 4) For communication initiated by LAN machines to INT, the IP addresses of the LAN machines should be translated to 123.123.1.200 at the router.

```
iptables -t nat -A POSTROUTING -o eth2 -s 192.168.1.0/24 -j SNAT --to-source 123.123.1.200
```

# 5) ICMP rules for INT and DMZ communications

# Allow INT to send/receive any ICMP message to/from DMZ

```
iptables -A FORWARD -i eth2 -o eth1 -p icmp -j ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -p icmp -j ACCEPT

# Delete the above rules
iptables -D FORWARD -i eth2 -o eth1 -p icmp -j ACCEPT
iptables -D FORWARD -i eth1 -o eth2 -p icmp -j ACCEPT

# Allow INT to send/receive ICMP ping requests (8) and responses (0) to/from DMZ
iptables -A FORWARD -i eth2 -o eth1 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -p icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -p icmp --icmp-type 0 -j ACCEPT

# Block all ICMP messages from DMZ to INT except for ping requests (8) and responses (0)
iptables -A FORWARD -i eth1 -o eth2 -p icmp -m icmp ! --icmp-type 8 -m icmp ! --icmp-type 0 -j DROP
```