```
#!/bin/bash
# Basic setup
# To clean up all defaults and existing rules
# Option "-F" indicates flush.

 iptables -F

# To make default policies (-p) to DROP for FORWARD and INPUT,
# and ACCEPT for OUTPUT.
# All the outgoing connections are allowed.

 iptables -P FORWARD DROP
 iptables -P OUTPUT ACCEPT
 iptables -P INPUT DROP

# Allow All Incoming SSH

 iptables -A INPUT  -i eth0 -p tcp --dport 22  -j ACCEPT
 iptables -A OUTPUT -o eth0 -p tcp --sport 22  -j ACCEPT

# Allow local loopback:
# from localhost to localhost without outgoing/incoming connections

 iptables -A INPUT  -i lo -j ACCEPT
 iptables -A OUTPUT -o lo -j ACCEPT

# Allow DNS (domain name server)
# To translate human-friendly computer hostnames into IP addresses
# e.g., www.hawaii.edu =  128.171.224.100

 iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT
 iptables -A INPUT  -p udp -i eth0 --sport 53 -j ACCEPT

# Allow ping from Inside (replying or receiving) to Outside (requesting)

 iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
 iptables -A INPUT  -p icmp --icmp-type echo-reply -j ACCEPT

# Allow Outgoing http

 iptables -A OUTPUT -o eth0 -p tcp --dport 80 \
          -m state --state NEW,ESTABLISHED -j ACCEPT

 iptables -A INPUT  -i eth0 -p tcp --sport 80 \
          -m state --state ESTABLISHED -j ACCEPT

# Allow Outgoing https

 iptables -A OUTPUT -o eth0 -p tcp --dport 443 \
          -m state --state NEW,ESTABLISHED -j ACCEPT

 iptables -A INPUT  -i eth0 -p tcp --sport 443 \
          -m state --state ESTABLISHED -j ACCEPT

# Printer (ipp=631, cups=515)

 iptables -A OUTPUT -p tcp -d 192.168.60.157  --dport 515 -j ACCEPT
 iptables -A INPUT  -p tcp -s 192.168.60.157  --sport 515 -j ACCEPT
```

```
# Preventing DoS attack (only for web server):
# 200 new connections (packets really) are allowed
# before the limit of 50 NEW connections (packets) per minute is applied.

 iptables -A INPUT -p tcp --dport 80 -m state --state NEW \
    -m limit --limit 50/minute --limit-burst 200 -j ACCEPT

# LOG
 iptables -A INPUT   -j LOG
 iptables -A FORWARD -j LOG

# Show the current iptables: -L indicates list.
 iptables -L
```