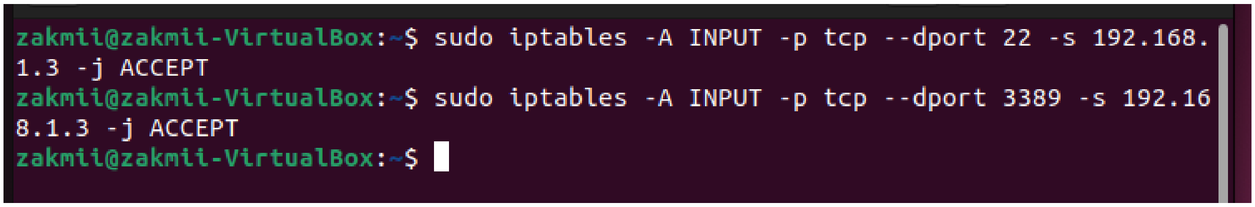
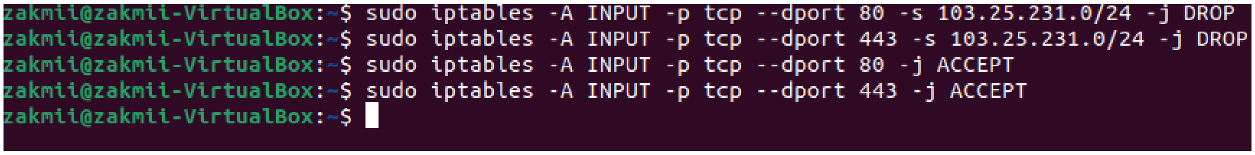
Allow only admin IPs(lets say 192.168.1.3) to access SSH/RDP.



```
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.
1.3 -j ACCEPT
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 3389 -s 192.16
8.1.3 -j ACCEPT
zakmii@zakmii-VirtualBox:~$
```

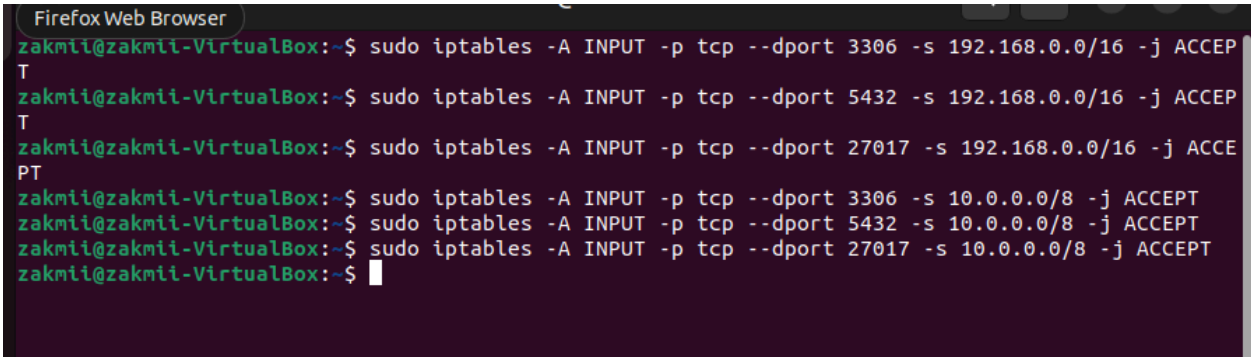
Allow HTTP/HTTPS but block access from blacklisted IP range 103.25.231.0/24.



```
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 80 -s 103.25.231.0/24 -j DROP
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 443 -s 103.25.231.0/24 -j DROP
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
zakmii@zakmii-VirtualBox:~$
```

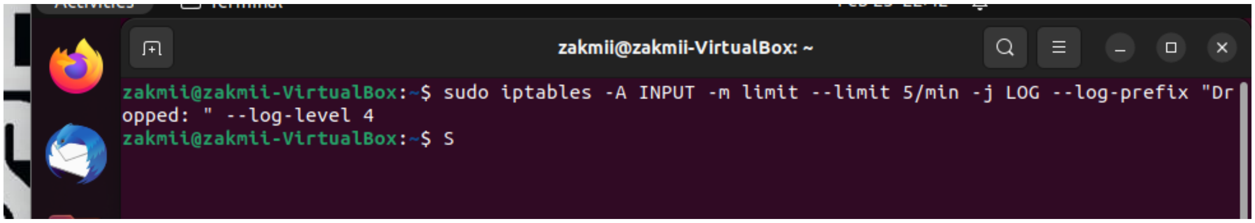
Allow only internal IPs to access the database server(consider default port for

databases).



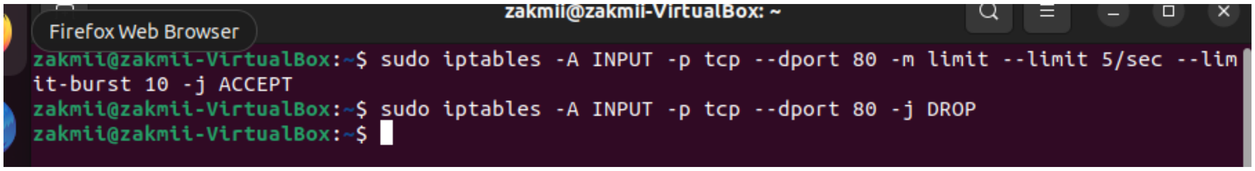
```
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 3306 -s 192.168.0.0/16 -j ACCEP
T
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 5432 -s 192.168.0.0/16 -j ACCEP
T
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 27017 -s 192.168.0.0/16 -j ACCE
PT
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 3306 -s 10.0.0.0/8 -j ACCEPT
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 5432 -s 10.0.0.0/8 -j ACCEPT
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 27017 -s 10.0.0.0/8 -j ACCEPT
zakmii@zakmii-VirtualBox:~$ 
```

Enable logging for debugging and tracking unauthorized access.



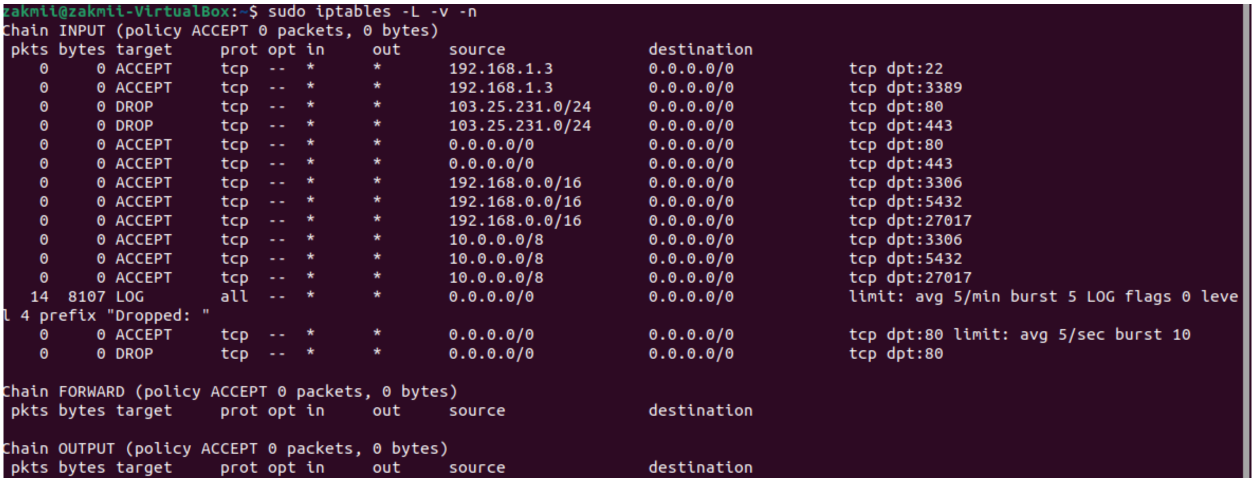
```
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "Dr
opped: " --log-level 4
zakmii@zakmii-VirtualBox:~$ S
```

Configure rate limiting to prevent excessive HTTP requests from a single IP.



```
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 80 -m limit --limit 5/sec --lim
it-burst 10 -j ACCEPT
zakmii@zakmii-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 80 -j DROP
zakmii@zakmii-VirtualBox:~$ 
```

Set a limit of 5 connections per second per IP to prevent overloading.



```
zakmii@zakmii-VirtualBox:~$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       192.168.1.3          0.0.0.0/0            tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       192.168.1.3          0.0.0.0/0            tcp dpt:3389
    0     0 DROP       tcp  --  *      *       103.25.231.0/24      0.0.0.0/0            tcp dpt:80
    0     0 DROP       tcp  --  *      *       103.25.231.0/24      0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     tcp  --  *      *       192.168.0.0/16       0.0.0.0/0            tcp dpt:3306
    0     0 ACCEPT     tcp  --  *      *       192.168.0.0/16       0.0.0.0/0            tcp dpt:5432
    0     0 ACCEPT     tcp  --  *      *       192.168.0.0/16       0.0.0.0/0            tcp dpt:27017
    0     0 ACCEPT     tcp  --  *      *       10.0.0.0/8           0.0.0.0/0            tcp dpt:3306
    0     0 ACCEPT     tcp  --  *      *       10.0.0.0/8           0.0.0.0/0            tcp dpt:5432
    0     0 ACCEPT     tcp  --  *      *       10.0.0.0/8           0.0.0.0/0            tcp dpt:27017
   14  8107 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0            limit: avg 5/min burst 5 LOG flags 0 leve
l 4 prefix "Dropped: "
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 limit: avg 5/sec burst 10
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```