Allow only admin IPs(lets say 192.168.1.3) to access SSH/RDP	1
Allow HTTP/HTTPS but block access from blacklisted IP range 103.25.231.0/24	1
Allow only internal IPs to access the database server(consider default port for	2
databases)	2
Enable logging for debugging and tracking unauthorized access	2
Configure rate limiting to prevent excessive HTTP requests from a single IP	2
Set a limit of 5 connections per second per IP to prevent overloading	2

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).

```
Firefox Web Browser

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:~$ 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:~ Q = - - ×

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:~

Firefox Web Browser
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 -\
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out
0 0 ACCEPT tcp -- * *
0 0 ACCEPT tcp -- * *
0 0 DROP tcp -- * *
                                                                                                                                       destination
                                                                                             source
                                                                                                                                      0.0.0.0/0
0.0.0.0/0
0.0.0.0/0
0.0.0.0/0
                                                                                                                                                                                 tcp dpt:22
tcp dpt:3389
tcp dpt:80
tcp dpt:443
                                                                                             192.168.1.3
                                                                                             192.168.1.3
103.25.231.0/24
                   0 DROP
                                             tcp
                                                                                             103.25.231.0/24
                                                                                            103.25.231.0/24

0.0.0.0/0

0.0.0.0/0

192.168.0.0/16

192.168.0.0/16

10.0.0.0/8

10.0.0.0/8

10.0.0.0/8
                                             tcp -- *
tcp -- *
                  0 ACCEPT
0 ACCEPT
0 ACCEPT
      0
                                                                                                                                       0.0.0.0/0
                                                                                                                                                                                 tcp dpt:80
                                                                                                                                                                                 tcp dpt:443
tcp dpt:3306
                                                                                                                                      0.0.0.0/0
0.0.0.0/0
                  0 ACCEPT
0 ACCEPT
0 ACCEPT
                                             tcp
                                                                                                                                       0.0.0.0/0
                                                                                                                                                                                 tcp dpt:5432
                                             tcp -- *
                                                                                                                                                                                 tcp dpt:3432
tcp dpt:27017
tcp dpt:3306
tcp dpt:5432
tcp dpt:27017
limit: avg 5/min burst 5 LOG flags 0 leve
                                                                                                                                      0.0.0.0/0
0.0.0.0/0
      0
  0 0 ACCEPT
0 0 ACCEPT
14 8107 LOG
4 prefix "Dropped: "
0 0 ACCEPT
0 0 DROP
                                                                                                                                      0.0.0.0/0
                                             tcp -- *
                                             tcp
all
                                                                                                                                       0.0.0.0/0
                                                                                            0.0.0.0/0
                                            tcp -- *
tcp -- *
                                                                                                                                                                                 tcp dpt:80 limit: avg 5/sec burst 10 tcp dpt:80
                                                                                            0.0.0.0/0
0.0.0.0/0
                                                                                                                                      0.0.0.0/0
0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out so
                                                                                                                                       destination
                                                                                            source
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source
                                                                                                                                       destination
```