Block Incoming Request From IP 1.2.3.4

The following command will drop any packet coming from the IP address 1.2.3.4:

Â /sbin/iptables -I INPUT -s {IP-HERE} -j DROP /sbin/iptables -I INPUT -s 1.2.3.4 -j DROP Â

You can also specify an interface such as eth1 via which a packet was received:

Â /sbin/iptables -I INPUT -i {INTERFACE-NAME-HERE} -s {IP-HERE} -j DROP
/sbin/iptables -I INPUT -i eth1 -s
1.2
.3
.4
-j DROP Â

Please note that when the "!" argument is used before the interface name, the sense is inverted:

Â /sbin/iptables -I INPUT ! -i {INTERFACE-NAME-HERE} -s {IP-HERE} -j DROP
/sbin/iptables -I INPUT ! -i eth1 -s
1.2
.3
.4
-j DROP Â

If the interface name ends in a "+", then any interface which begins with this name will match. If this option is omitted, any interface name will match:

Â /sbin/iptables -I INPUT -i {INTERFACE-NAME-HERE}+ -s {IP-HERE} -j DROP
/sbin/iptables -I INPUT -i br+ -s
1.2
.3
.4
-j DROP Â

You can replace -I INPUT (insert) with -A INPUT (append) rule as follows:

Â /sbin/iptables -A INPUT -s 1.2.3.4 -j DROP /sbin/iptables -i eth1 -A INPUT -s 1.2.3.4 -j DROP Â

How Do I Block Subnet (xx.yy.zz.ww/ss)?

Use the following syntax to block 10.0.0.0/8 on eth1 public interface:
/sbin/iptables -i eth1 -A INPUT -s 10.0.0.0/8 -j DROP

How Do I Block and Log Dropped IP Address Information?

You can turn on kernel logging of matching packets with LOG target as follows:
/sbin/iptables -i eth1 -A INPUT -s 10.0.0.0/8 -j LOG --log-prefix "IP DROP SPOOF A:"
The next rule will actually drop the ip / subnet:
/sbin/iptables -i eth1 -A INPUT -s 10.0.0.0/8 -j DROP

How Do I View Blocked IP Address?

Simply use the following command:
/sbin/iptables -L -v
OR
/sbin/iptables -L INPUT -v
OR
/sbin/iptables -L INPUT -v -n
Sample outputs:

Chain INPUT (policy ACCEPT 3107K packets, 1847M bytes) pkts bytes target prot opt in out source destination 0 0 DROP all -- br+ any 1.2.3.4 anywhere 0 0 DROP all -- !eth1 any 1.2.3.4 anywhere 0 0 DROP all -- !eth1 any 1.2.3.4 anywhere

How Do I Search For Blocked IP Address?

Use the grep command as follows:
/sbin/iptables -L INPUT -v -n | grep 1.2.3.4

How Do I Delete Blocked IP Address?

First, you need to display blocked IP address along with line number and other information, enter:
iptables -L INPUT -n --line-numbers
iptables -L INPUT -n --line-numbers | grep 1.2.3.4
Sample outputs:

num pkts bytes target prot opt in out source destination 1 0 0 DROP

0 -- * * 116.199.128.1 0.0.0.0/0 2 0 0 DROP 0 -- * * 116.199.128.10 0.0.0.0/0 3 0 0 DROP 0 -- * * 123.199.2.255 0.0.0.0/0

To delete line number 3 (123.199.2.255), enter:
iptables -D INPUT 3
Verify the same, enter:
iptables -L INPUT -v -n
You can also use the following syntax:
iptables -D INPUT -s 1.2.3.4 -j DROP

How Do I Save Blocked IP Address?

If you are using Redhat / RHEL / CentOS / Fedora Linux, type the following command:
iptables -D INPUT -s 1.2.3.4 -j DROP
##########################
#////// command to save iptables ///////#
##########################
/sbin/service iptables save
less /etc/sysconfig/iptables
grep '1.2.3.4' /etc/sysconfig/iptables
For all **other Linux distributions** use the iptables-save command to dump the contents of an IP Table to a file:
iptables-save > /root/myfirewall.conf
Please not that you need to run the 'iptables-save' or 'service iptables save' as soon as you add or delete the ip address.

A Note About Restoring Firewall

To restore your firewall use the iptables-restore command to restore IP Tables from a file called /root/myfirewall.conf, enter:
iptables-restore

How Do I Block Large Number Of IP Address or Subnets?

You need to write a shell script as follows:

#!/bin/bash _input="/root/blocked.ip.db" IPT=/sbin/iptables $IPT -N droplist egrep -v "^#|^$" x |
while
IFS=
read
-r ip

```
do

$IPT
-A droplist -i eth1 -s
$ip
-j LOG --log-prefix
"IP BlockList "

$IPT
-A droplist -i eth1 -s
$ip
-j DROP
done
"$_input"

# Drop it

$IPT
-I INPUT -j droplist
$IPT
-I OUTPUT -j droplist
$IPT
-I FORWARD -j droplist
```

See also: iptables: Read a List of IP Address From File And Block

Block Outgoing Request From LAN IP 192.168.1.200?

Use the following syntax:
/sbin/iptables -A OUTPUT -s 192.168.1.200 -j DROP
/sbin/service iptables save
You can also use FORWARD default chainswhen packets send through another interface. Usually FORWARD used when you setup Linux as a router:
/sbin/iptables -A FORWARD -s 192.168.1.200 -j DROP
/sbin/service iptables save