In the above example:

- -m limit: This uses the limit iptables extension
- –limit 25/minute: This limits only maximum of 25 connection per minute. Change this value based on your specific requirement
- –limit-burst 100: This value indicates that the limit/minute will be enforced only after the total number of connection have reached the limit-burst level.

24. Port Forwarding

The following example routes all traffic that comes to the port 442 to 22. This means that the incoming ssh connection can come from both port 22 and 422.

```
iptables -t nat -A PREROUTING -p tcp -d 192.168.102.37 --dport 422 -j DNAT --to 192.168.102.37:22
```

If you do the above, you also need to explicitly allow incoming connection on the port 422.

```
iptables -A INPUT -i eth0 -p tcp --dport 422 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 422 -m state --state ESTABLISHED -j ACCEPT
```

25. Log Dropped Packets

You might also want to log all the dropped packets. These rules should be at the bottom.

First, create a new chain called LOGGING.

```
iptables -N LOGGING
```

Next, make sure all the remaining incoming connections jump to the LOGGING chain as shown below.

```
iptables -A INPUT -j LOGGING
```

Next, log these packets by specifying a custom “log-prefix”.

```
iptables -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "IPTables Packet Dropped: " --log-level 7
```

Finally, drop these packets.

```
iptables -A LOGGING -j DROP
```

All of the above 25 iptables rules are in shell script format: iptables-rules

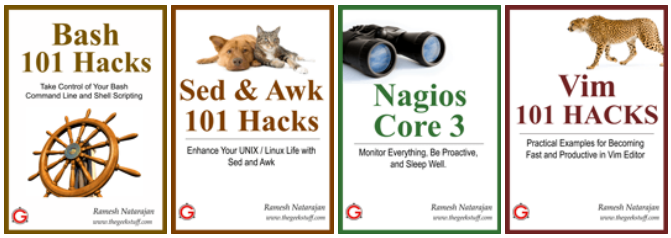
Previous articles in the iptables series:

- Linux Firewall Tutorial: IPTables Tables, Chains, Rules Fundamentals
- IPTables Flush: Delete / Remove All Rules On RedHat and CentOS Linux
- Linux IPTables: How to Add Firewall Rules (With Allow SSH Example)
- Linux IPTables: Incoming and Outgoing Rule Examples (SSH and HTTP)

If you enjoyed this article, you might also like..

1. 50 Linux Sysadmin Tutorials
2. 50 Most Frequently Used Linux Commands (With Examples)
3. Top 25 Best Linux Performance Monitoring and Debugging Tools
4. Mommy, I found it! – 15 Practical Linux Find Command Examples
5. Linux 101 Hacks 2nd Edition eBook Free

- Awk Introduction – 7 Awk Print Examples
- Advanced Sed Substitution Examples
- 8 Essential Vim Editor Navigation Fundamentals
- 25 Most Frequently Used Linux IPTables Rules Examples
- Turbocharge PuTTY with 12 Powerful Add-Ons



Tagged as: IPTables Block IP, IPTables Block IP Address, IPTables Block Port, IPTables DNAT, IPTables HowTo, IPTables Log, IPTables NAT, IPTables Tutorial, IPTables Ubuntu

{ 50 comments… add one }

- kgas June 14, 2011, 3:42 am

  Good one and expecting all your iptables related writings in a single pdf file. Thanks

  Link
- diptanu June 14, 2011, 3:57 am

  Hi,Thanks alot for the above info.However would like to know that if the blocking or allowing through iptables is possible for specific MAC address over internet, as because if my eth0 is using a local ip 10.10.10.10 which is natted via public ip eg 100.100.100.100 and connected to internet via ISP, then someone from internet with specific MAC id (allowed in iptables) should be able to ssh to my public ip (100.100.100.100) and the rest should be dropped.

  Is that possible over the internet