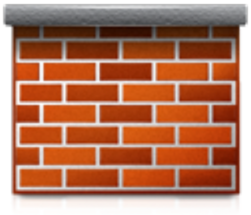
nixCraft

Linux / Unix tutorials for new and seasoned sysadmin || developers

How to list all iptables rules with line numbers on Linux

Author: Vivek Gite • Last updated: December 30, 2020 • 4 comments



I recently added NAT rules on my RHEL 6.x system. How do I see the rules including line numbers that I just added in Linux?

Yes, you can easily **list all iptables rules using the following commands** on Linux:

1) **iptables command** – IPv4 netfilter admin tool to display

iptables firewall rules.

2) **ip6tables command** – IPv6 netfilter admin tool to show rules.

How to list all iptables rules on Linux

The procedure to list all rules on Linux is as follows:

1. Open the terminal app or login using ssh:

   ```
   ssh user@server-name
   ```

2. To list all IPv4 rules :

   ```
   sudo iptables -S
   ```

3. To list all IPv6 rules :

   ```
   sudo ip6tables -S
   ```

4. To list all tables rules :

   ```
   sudo iptables -L -v -n | more
   ```

5. To list all rules for INPUT tables :

   ```
   sudo iptables -L INPUT -v -n
   ```

```
sudo iptables -S INPUT
```

Let us see all syntax and usage in details to show and list all iptables rules on Linux operating systems.

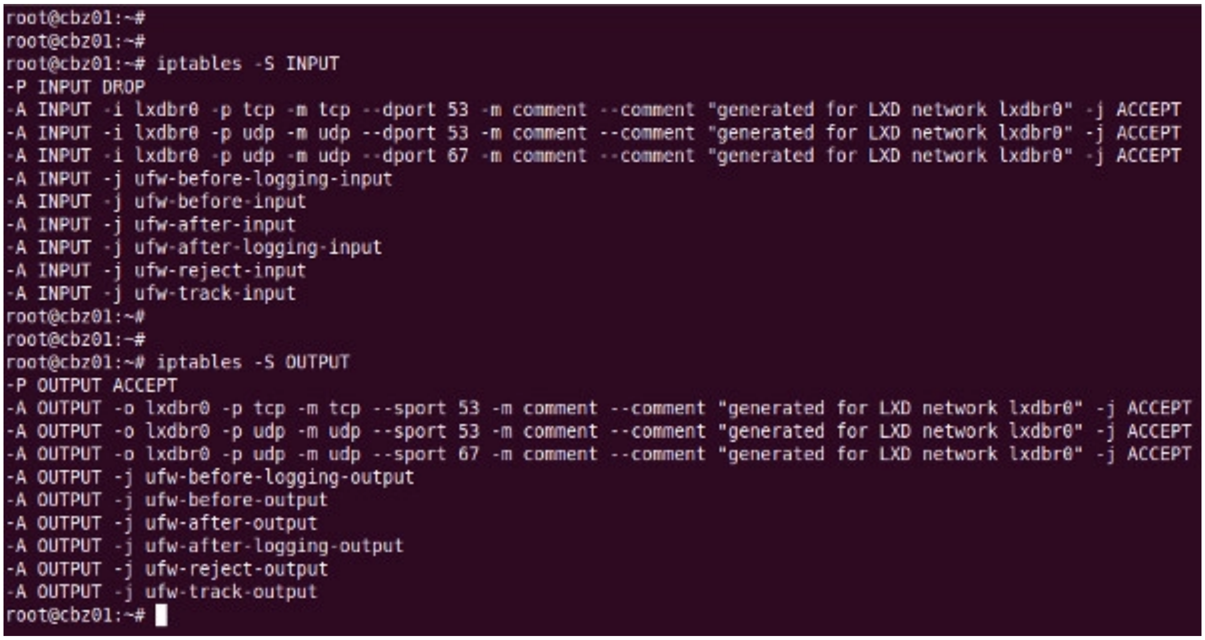
Viewing all iptables rules in Linux

The syntax is:

```
iptables -S
iptables --list
iptables -L
iptables -S TABLE_NAME
iptables --table NameHere --list
iptables -t NameHere -L -n -v --line-numbers
```

Print all rules in the selected chain

```
sudo iptables -S
sudo iptables -S INPUT
iptables -S OUTPUT
```



```
root@cbz01:~#
root@cbz01:~#
root@cbz01:~# iptables -S INPUT
-P INPUT DROP
-A INPUT -i lxdbr0 -p tcp -m tcp --dport 53 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A INPUT -i lxdbr0 -p udp -m udp --dport 53 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A INPUT -i lxdbr0 -p udp -m udp --dport 67 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A INPUT -j ufw-before-logging-input
-A INPUT -j ufw-before-input
-A INPUT -j ufw-after-input
-A INPUT -j ufw-after-logging-input
-A INPUT -j ufw-reject-input
-A INPUT -j ufw-track-input
root@cbz01:~#
root@cbz01:~#
root@cbz01:~# iptables -S OUTPUT
-P OUTPUT ACCEPT
-A OUTPUT -o lxdbr0 -p tcp -m tcp --sport 53 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A OUTPUT -o lxdbr0 -p udp -m udp --sport 53 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A OUTPUT -o lxdbr0 -p udp -m udp --sport 67 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A OUTPUT -j ufw-before-logging-output
-A OUTPUT -j ufw-before-output
-A OUTPUT -j ufw-after-output
-A OUTPUT -j ufw-after-logging-output
-A OUTPUT -j ufw-reject-output
-A OUTPUT -j ufw-track-output
root@cbz01:~#
```

How to list rules for given tables

Type the following command as root user:

```
# iptables -L INPUT
# iptables -L FORWARD
# iptables -L OUTPUT
# iptables -L
```

Sample outputs:

```
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:bootps
ACCEPT     udp  --  anywhere             anywhere             udp dpt:bootps
ufw-before-logging-input  all  --  anywhere             anywhere
ufw-before-input  all  --  anywhere             anywhere
ufw-after-input  all  --  anywhere             anywhere
ufw-after-logging-input  all  --  anywhere             anywhere
ufw-reject-input  all  --  anywhere             anywhere
ufw-track-input  all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ufw-before-logging-forward  all  --  anywhere             anywhere
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere
ufw-after-logging-forward  all  --  anywhere             anywhere
ufw-reject-forward  all  --  anywhere             anywhere
ufw-track-forward  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-output  all  --  anywhere             anywhere
ufw-before-output  all  --  anywhere             anywhere
ufw-after-output  all  --  anywhere             anywhere
ufw-after-logging-output  all  --  anywhere             anywhere
ufw-reject-output  all  --  anywhere             anywhere
ufw-track-output  all  --  anywhere             anywhere
.....
..
..
Chain ufw-user-limit (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 5 LO
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-unrea

Chain ufw-user-limit-accept (0 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain ufw-user-logging-forward (0 references)
target     prot opt source               destination

Chain ufw-user-logging-input (0 references)
```

```
target     prot opt source               destination

Chain ufw-user-logging-output (0 references)
target     prot opt source               destination

Chain ufw-user-output (1 references)
target     prot opt source               destination
```

Let us try to understand rules:

- **target** – Tell what to down when a packet matches the rule.
- **prot** – The protocol for rule.
- **opt** – Additional options for rule.
- **source** – The source IP address/subnet/domain name.
- **destination** – The destination IP address/subnet/domain name.

How to see nat rules:

By default the `filter` table is used. To see NAT rules, enter:

```
# iptables -t nat -L
```

Other table options:

```
# iptables -t filter -L
# iptables -t raw -L
# iptables -t security -L
# iptables -t mangle -L
# iptables -t nat -L
```

How to see nat rules with line numbers:

Pass the `--line-numbers` option:

```
# iptables -t nat -L --line-numbers -n
```

Sample outputs:

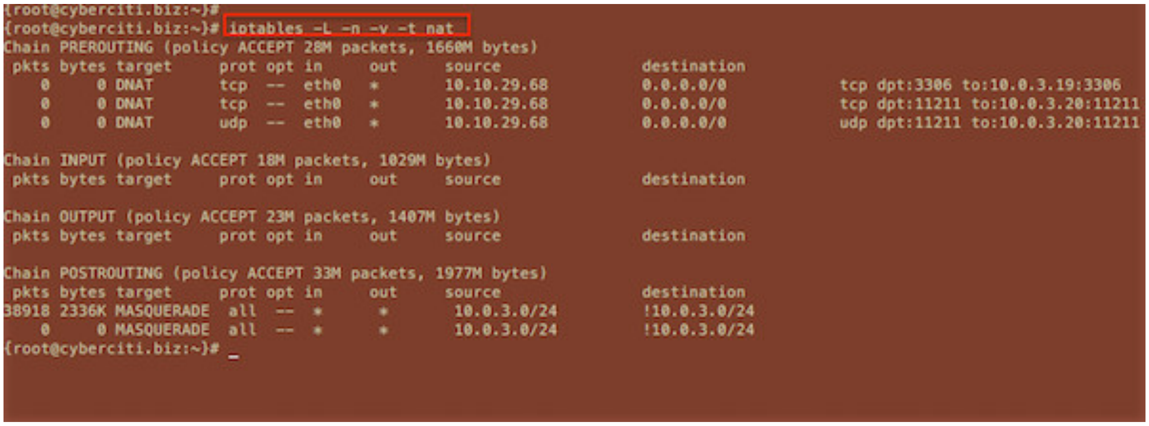
```
Chain PREROUTING (policy ACCEPT 28M packets, 1661M bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DNAT       tcp  --  eth0   *       10.10.29.68          0.0.0.0/0
2        0     0 DNAT       tcp  --  eth0   *       10.10.29.68          0.0.0.0/0
3        0     0 DNAT       udp  --  eth0   *       10.10.29.68          0.0.0.0/0

Chain INPUT (policy ACCEPT 18M packets, 1030M bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 23M packets, 1408M bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 33M packets, 1979M bytes)
num   pkts bytes target     prot opt in     out     source               destination
1    38927 2336K MASQUERADE  all  --  *      *       10.0.3.0/24         !10.0.3.0/24
2        0     0 MASQUERADE  all  --  *      *       10.0.3.0/24         !10.0.3.0/24
```

How to see nat rules with counters (bytes and packets)

Pass the `-v` option to iptables command to view all iptables rules on Linux:

```
# iptables -t nat -L -n -v
```

Sample outputs:



```
{root@cyberciti.biz:~}#
{root@cyberciti.biz:~}# iptables -L -n -v -t nat
Chain PREROUTING (policy ACCEPT 28M packets, 1660M bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp  --  eth0   *       10.10.29.68          0.0.0.0/0           tcp dpt:3306 to:10.0.3.19:3306
    0     0 DNAT       tcp  --  eth0   *       10.10.29.68          0.0.0.0/0           tcp dpt:11211 to:10.0.3.20:11211
    0     0 DNAT       udp  --  eth0   *       10.10.29.68          0.0.0.0/0           udp dpt:11211 to:10.0.3.20:11211

Chain INPUT (policy ACCEPT 18M packets, 1029M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 23M packets, 1407M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 33M packets, 1977M bytes)
 pkts bytes target     prot opt in     out     source               destination
38918 2336K MASQUERADE  all  --  *      *       10.0.3.0/24         !10.0.3.0/24
    0     0 MASQUERADE  all  --  *      *       10.0.3.0/24         !10.0.3.0/24
{root@cyberciti.biz:~}# _
```

Fig.01: Linux viewing all iptables NAT, DNAT, MASQUERADE rules

Say hello to ip6tables

ip6tables is administration tool for IPv6 packet filtering and NAT. To see IPv6 tables, enter:

```
# ip6tables -L -n -v
```

```
Chain INPUT (policy DROP 239 packets, 16202 bytes)
 pkts bytes target     prot opt in     out     source
 136K   30M ufw6-before-logging-input  all      *      *       ::/0
 136K   30M ufw6-before-input  all      *      *       ::/0
  241 16360 ufw6-after-input  all      *      *       ::/0
  239 16202 ufw6-after-logging-input  all      *      *       ::/0
  239 16202 ufw6-reject-input  all      *      *       ::/0
  239 16202 ufw6-track-input  all      *      *       ::/0

Chain FORWARD (policy DROP 483 packets, 32628 bytes)
 pkts bytes target     prot opt in     out     source
  483 32628 ufw6-before-logging-forward  all      *      *       ::
  483 32628 ufw6-before-forward  all      *      *       ::/0
  483 32628 ufw6-after-forward  all      *      *       ::/0
  483 32628 ufw6-after-logging-forward  all      *      *       ::/
  483 32628 ufw6-reject-forward  all      *      *       ::/0
  483 32628 ufw6-track-forward  all      *      *       ::/0

Chain OUTPUT (policy ACCEPT 122 packets, 8555 bytes)
 pkts bytes target     prot opt in     out     source
 136K   30M ufw6-before-logging-output  all      *      *       ::/
 136K   30M ufw6-before-output  all      *      *       ::/0
  183 14107 ufw6-after-output  all      *      *       ::/0
  183 14107 ufw6-after-logging-output  all      *      *       ::/0
  183 14107 ufw6-reject-output  all      *      *       ::/0
  183 14107 ufw6-track-output  all      *      *       ::/0

Chain ufw6-after-forward (1 references)
 pkts bytes target     prot opt in     out     source

...
....
..
 pkts bytes target     prot opt in     out     source
   19  1520 ACCEPT     tcp      *      *       ::/0
   42  4032 ACCEPT     udp      *      *       ::/0

Chain ufw6-user-forward (1 references)
```

```
 pkts bytes target     prot opt in     out     source

Chain ufw6-user-input (1 references)
 pkts bytes target     prot opt in     out     source

Chain ufw6-user-limit (0 references)
 pkts bytes target     prot opt in     out     source
    0     0 LOG        all      *      *       ::/0
level 4 prefix "[UFW LIMIT BLOCK] "
    0     0 REJECT     all      *      *       ::/0

Chain ufw6-user-limit-accept (0 references)
 pkts bytes target     prot opt in     out     source
    0     0 ACCEPT     all      *      *       ::/0

Chain ufw6-user-logging-forward (0 references)
 pkts bytes target     prot opt in     out     source

Chain ufw6-user-logging-input (0 references)
 pkts bytes target     prot opt in     out     source

Chain ufw6-user-logging-output (0 references)
 pkts bytes target     prot opt in     out     source

Chain ufw6-user-output (1 references)
 pkts bytes target     prot opt in     out     source
```

To see nat rules and line-numbers, enter:

```
# ip6tables -L -n -v -t nat --line-numbers
```

Conclusion

You learned how to display, filter and list all iptables rules on Linux system using the CLI. See iptables man pages by typing the following man command:

```
$ man iptables
$ man ip6tables
```

UP NEXT

Linux Network IP Accounting

CentOS / Redhat Iptables Firewall Configuration Tutorial

How to add comments to iptables rules on Linux

CentOS / RHEL IPv6 ip6tables Firewall Configuration

Linux: Iptables List and Show All NAT IPTables Rules Command

How to install Composer on Debian / Ubuntu Linux

Iptables insert rule at top of tables (PREPEND rule on Linux)

Category	List of Unix and Linux commands
File Management	cat
Firewall	Alpine Awall • CentOS 8 • OpenSUSE • RHEL 8 • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 20.04
Network Utilities	dig • host • ip • nmap
OpenVPN	CentOS 7 • CentOS 8 • Debian 10 • Debian 8/9 • Ubuntu 18.04 • Ubuntu 20.04
Package Manager	apk • apt
Processes Management	bg • chroot • cron • disown • fg • jobs • killall • kill • pidof • pstree • pwdx • time

Category	List of Unix and Linux commands
Searching	grep • whereis • which
User Information	groups • id • lastcomm • last • lid/libuser-lid • logname • members • users • whoami • who • w
WireGuard VPN	Alpine • CentOS 8 • Debian 10 • Firewall • Ubuntu 20.04

4 comments… add one ↓

TJ • Jan 22, 2018 @ 17:03

Thanks you it saved me tons of time.

reply link

Carlos • Oct 5, 2020 @ 10:12

I was looking to display the iptables rules in the table view as I needed to compare different rules against each other. It solved my problem

```
iptables -L
```

Gracias

reply link

tedmar • Oct 5, 2020 @ 22:08

Yehh, thank you

reply link

Feebee • Dec 30, 2020 @ 15:18

Yes, I wanted to list and delete my iptables firewall rules. this was very useful.

reply link

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

Use HTML <pre>...</pre> for code samples. Problem posting comment? Email me @ webmaster@cyberciti.biz

Next FAQ: How to undefine and unset a bash environment variable on Linux or Unix

Previous FAQ: How to check boot path (partition) in Linux

Featured Articles

1 30 Cool Open Source Software I Discovered in 2013

2 30 Handy Bash Shell Aliases For Linux / Unix / Mac OS X

3 Top 32 Nmap Command Examples For Linux Sys/Network Admins

4 25 PHP Security Best Practices For Linux Sys Admins

5 30 Linux System Monitoring Tools Every SysAdmin Should Know

6. 40 Linux Server Hardening Security Tips

7. Linux: 25 Iptables Netfilter Firewall Examples For New SysAdmins

8. Top 20 OpenSSH Server Best Security Practices

9. Top 25 Nginx Web Server Best Security Practices

10. My 10 UNIX Command Line Mistakes