

How to Enable Logging in Iptables on Linux

Written by [Rahul](#), Updated on September 26, 2019

🔥 firewall, iptables, logging

Enabling logging on iptables is helpful for monitoring traffic coming to our server. This we can also find the number of hits done from any IP. This article will help enable logging in iptables for all packets filtered by iptables.

Enable Iptables LOG

We can simply use following command to enable logging in iptables.

```
$ iptables -A INPUT -j LOG
```

We can also define the source ip or range for which log will be created.

```
$ iptables -A INPUT -s 192.168.10.0/24 -j LOG
```

To define level of LOG generated by iptables us `--log-level` followed by level number.

```
$ iptables -A INPUT -s 192.168.10.0/24 -j LOG --log-level 4
```

We can also add some prefix in generated Logs. So it will be easy to search for logs in a huge file.

```
$ iptables -A INPUT -s 192.168.10.0/24 -j LOG --log-prefix '** SUSPECT **'
```

View Iptables LOG

After enabling iptables logs. check following log files to view logs generated by iptables as per your operating system.

On Ubuntu and Debian

iptables logs are generated by the kernel. So check following kernel log file.

```
$ tail -f /var/log/kern.log
```

On CentOS/RHEL and Fedora

```
$ cat /var/log/messages
```

Change Iptables LOG File Name

To change iptables log file name edit `/etc/rsyslog.conf` file and add following configuration in file.

```
$ vi /etc/syslog.conf
```

Add the following line

```
kern.warning /var/log/iptables.log
```

Now, restart rsyslog service using the following command.

```
$ service rsyslog restart
```

SHARE IT!



RAHUL








I, Rahul Kumar am the founder and chief editor of TecAdmin.net. I am a Red Hat Certified Engineer (RHCE) and working as an IT professional since 2009..

RELATED POSTS

- **What is FirewallD And How To Implement On Linux**
March 19, 2020
- **How to Enable PHP errors to Display on Web Browser**
January 23, 2019
- **How to Enable CSF Firewall Web UI**
August 5, 2017
- **How to Install and Configure CSF Firewall on Linux**
November 19, 2015
- **How To Setup UFW Firewall on Ubuntu and Debian**
September 8, 2015

6 COMMENTS

- **BHUSHIT**
November 19, 2019 at 6:18 am
Hi All,
I want to log the NAT translations(source NAT) along with the timestamps. Info I want is:
source IP(unnatted) source port dest IP dest port :: source IP(natted) source port dest IP dest port

Please help me if its possible.
- **ZER00COOL**
September 23, 2019 at 9:12 pm
Change :
tailf /var/log/kern.log
by
tail -f /var/log/kern.log
- **HENRIQUE**
November 22, 2017 at 7:35 pm
If you have difficulty to log packets with anothers rules, use "iptables -I" instead of "-A", this put your logging rule at top of rules. Netfilter matches others rules and stop processing, but LOG is a non-blocking target, it's secure to put in first place.
- **DON**
November 7, 2017 at 11:35 am
Great post thank you
- **NAME**
April 23, 2016 at 10:46 pm
Not very flexible youre solution.

Better try this

nano /etc/rsyslog.d/iptables.conf


add this:
"msg.contains,** SUSPECT **" /var/log/iptables.log
&~

"
without the quotes ofc

then

service rsyslog restart

done

cheers
- **ROB FREEMAN**
March 18, 2016 at 9:14 pm
Thanks for the information here. Just wanted to let you know, there is a type on one line.

vi /etc/syslog.conf

This should be

vi /etc/rsyslog.conf

LEAVE A REPLY

COMMENTS *

NAME *

EMAIL *

WEBSITE

☐ SAVE MY NAME, EMAIL, AND WEBSITE IN THIS BROWSER FOR THE NEXT TIME I COMMENT.

☐ Je ne suis pas un robot

reCAPTCHA
Confidentialité - Conditions

SUBMIT

Search Now

POPULAR POSTS

How to Install Apache, MySQL & PHP on Ubuntu 20.04

How to install Apache, MySQL & PHP (LAMP) on CentOS 8

How to Install PHP on Ubuntu 20.04

How to Install Laravel on Ubuntu 20.04

How to Check IP Address on Ubuntu 20.04 (Desktop)