Модули Iptables

НЕ РЕШЕНО

Грузим модуль modprobe

Потом прописываем в :

For iptables on CentOS there is an additional location which is where I have those particular modules configured to load and that's the /etc/sysconfig/iptables-config file. The start of the file looks like this

# Load additional iptables modules (nat helpers)

# Default: -none-

# Space separated list of nat helpers (e.g. 'ip\_nat\_ftp ip\_nat\_irc'), which

# are loaded after the firewall rules are applied. Options for the helpers are

# stored in /etc/modprobe.conf.

IPTABLES\_MODULES="nf\_conntrack\_ftp nf\_conntrack"

When I run service iptables restart I get this line

Loading additional iptables modules: nf\_conntrack\_ftp nf\_

[**IPTables. Setting nf\_log kernel parameter**](https://forums.centos.org/viewtopic.php?t=54411#p230026)

* [**Quote**](https://forums.centos.org/posting.php?mode=quote&f=47&p=230026&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)

[Post](https://forums.centos.org/viewtopic.php?p=230026&sid=3ed01ed0c5af6da52a82b9b9a0996ad0#p230026) by **[Annm](https://forums.centos.org/memberlist.php?mode=viewprofile&u=100426&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)** » 2015/09/30 07:55:48

SELinux: disabled  
  
I want to be able to track how packets processed through IPTables rules using "TRACE" target.  
  
For example:  
iptables -t raw -A PREROUTING -s 192.168.1.0/24 -d 192.168.2.0/24 -j TRACE.  
  
In order to do this I need to set kernel parameter et.netfilter.nf\_log.2 to xt\_LOG, but I can't:

**CODE:**[**SELECT ALL**](https://forums.centos.org/viewtopic.php?t=54411)

[root@srv nf\_log]# sysctl -a | grep nf\_log

net.netfilter.nf\_log.0 = NONE

net.netfilter.nf\_log.1 = NONE

net.netfilter.nf\_log.10 = NONE

net.netfilter.nf\_log.11 = NONE

net.netfilter.nf\_log.12 = NONE

net.netfilter.nf\_log.2 = NONE

net.netfilter.nf\_log.3 = NONE

net.netfilter.nf\_log.4 = NONE

net.netfilter.nf\_log.5 = NONE

net.netfilter.nf\_log.6 = NONE

net.netfilter.nf\_log.7 = NONE

net.netfilter.nf\_log.8 = NONE

net.netfilter.nf\_log.9 = NONE

[root@srv nf\_log]# lsmod| grep xt\_LOG

[root@srv nf\_log]# modprobe xt\_LOG

[root@srv nf\_log]# lsmod| grep xt\_LOG

xt\_LOG 12690 0

[root@srv nf\_log]# sysctl net.netfilter.nf\_log.2=xt\_LOG

sysctl: setting key "net.netfilter.nf\_log.2": No such file or directory

net.netfilter.nf\_log.2 = xt\_LOG

[root@srv nf\_log]# echo xt\_LOG > /proc/sys/net/netfilter/nf\_log/2

bash: echo: write error: No such file or directory

[root@srv nf\_log]# ls -l /proc/sys/net/netfilter/nf\_log/

total 0

-rw-r--r-- 1 root root 0 Sep 29 19:27 0

-rw-r--r-- 1 root root 0 Sep 29 19:23 1

-rw-r--r-- 1 root root 0 Sep 29 19:23 10

-rw-r--r-- 1 root root 0 Sep 29 19:23 11

-rw-r--r-- 1 root root 0 Sep 29 19:23 12

-rw-r--r-- 1 root root 0 Sep 29 19:24 2

-rw-r--r-- 1 root root 0 Sep 29 19:23 3

-rw-r--r-- 1 root root 0 Sep 29 19:23 4

-rw-r--r-- 1 root root 0 Sep 29 19:23 5

-rw-r--r-- 1 root root 0 Sep 29 19:23 6

-rw-r--r-- 1 root root 0 Sep 29 19:23 7

-rw-r--r-- 1 root root 0 Sep 29 19:23 8

-rw-r--r-- 1 root root 0 Sep 29 19:23 9

So, as you can see, sysctl complains about missing file or directory, while they exist.  
  
I don't have this problem with Centos 6. Would appreciate any advice.

Last edited by [Annm](https://forums.centos.org/memberlist.php?mode=viewprofile&u=100426&sid=3ed01ed0c5af6da52a82b9b9a0996ad0) on 2015/10/01 11:04:25, edited 1 time in total.

[Top](https://forums.centos.org/viewtopic.php?t=54411#top)

[**Annm**](https://forums.centos.org/memberlist.php?mode=viewprofile&u=100426&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)

Posts: [2](https://forums.centos.org/search.php?author_id=100426&sr=posts&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)

Joined: 2015/09/30 07:44:29

[**Re: Setting nf\_log kernel parameter fails**](https://forums.centos.org/viewtopic.php?t=54411#p230099)

* [**Quote**](https://forums.centos.org/posting.php?mode=quote&f=47&p=230099&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)

[Post](https://forums.centos.org/viewtopic.php?p=230099&sid=3ed01ed0c5af6da52a82b9b9a0996ad0#p230099) by **[Annm](https://forums.centos.org/memberlist.php?mode=viewprofile&u=100426&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)** » 2015/10/01 11:02:26

Any help? Does nobody use TRACE target? I think it's such a vital feature, somebody must know what's wrong with my setup.

[Top](https://forums.centos.org/viewtopic.php?t=54411#top)

[**mihaig11**](https://forums.centos.org/memberlist.php?mode=viewprofile&u=100857&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)

Posts: [1](https://forums.centos.org/search.php?author_id=100857&sr=posts&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)

Joined: 2015/10/23 10:14:25

[**Re: IPTables. Setting nf\_log kernel parameter**](https://forums.centos.org/viewtopic.php?t=54411#p231339)

* [**Quote**](https://forums.centos.org/posting.php?mode=quote&f=47&p=231339&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)

[Post](https://forums.centos.org/viewtopic.php?p=231339&sid=3ed01ed0c5af6da52a82b9b9a0996ad0#p231339) by [**mihaig11**](https://forums.centos.org/memberlist.php?mode=viewprofile&u=100857&sid=3ed01ed0c5af6da52a82b9b9a0996ad0) » 2015/10/23 12:24:55

I think they split the xt\_LOG code in newer kernel versions and you need to modprobe nf\_log\_ipv4 now and sysctl net.netfilter.nf\_log.2=nf\_log\_ipv4 (assuming you want to trace ipv4 packets)

[Top](https://forums.centos.org/viewtopic.php?t=54411#top)

[**bronson**](https://forums.centos.org/memberlist.php?mode=viewprofile&u=101659&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)

Posts: [1](https://forums.centos.org/search.php?author_id=101659&sr=posts&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)

Joined: 2015/12/03 08:19:34

[**Re: IPTables. Setting nf\_log kernel parameter**](https://forums.centos.org/viewtopic.php?t=54411#p233626)

* [**Quote**](https://forums.centos.org/posting.php?mode=quote&f=47&p=233626&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)

[Post](https://forums.centos.org/viewtopic.php?p=233626&sid=3ed01ed0c5af6da52a82b9b9a0996ad0#p233626) by **[bronson](https://forums.centos.org/memberlist.php?mode=viewprofile&u=101659&sid=3ed01ed0c5af6da52a82b9b9a0996ad0)** » 2015/12/03 08:24:31

You're right. Plus kernel logging is disabled by default in Centos 7. I had to modify /etc/rsyslog.conf and `systemctl restart rsyslog` before the log messages would show up.

Для работы сценария [rc.firewall.txt](https://www.opennet.ru/docs/RUS/iptables/#RCFIREWALLTXT) вам необходимо будет добавить в ядро следующие опции или собрать соответствующие подгружаемые модули. За информацией по опциям, необходимым для работы других сценариев, обращайтесь к приложению с примерами этих сценариев.

* CONFIG\_PACKET
* CONFIG\_NETFILTER
* CONFIG\_IP\_NF\_CONNTRACK
* CONFIG\_IP\_NF\_FTP
* CONFIG\_IP\_NF\_IRC
* CONFIG\_IP\_NF\_IPTABLES
* CONFIG\_IP\_NF\_FILTER
* CONFIG\_IP\_NF\_NAT
* CONFIG\_IP\_NF\_MATCH\_STATE
* CONFIG\_IP\_NF\_TARGET\_LOG
* CONFIG\_IP\_NF\_MATCH\_LIMIT
* CONFIG\_IP\_NF\_TARGET\_MASQUERADE