

Table Of Contents

Table Of Contents 1

iptables geoip patch 3

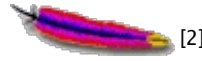
[Home](#) > [Faq](#) > [CentOS](#)

Linux Iptables Just Block By Country

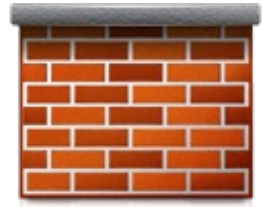
Posted by [Vivek Gite](#) <vivek@nixcraft.com>

I admin ecom website and a lot of bogus traffic comes from countries that do not offer much in commercial value. How do I just configure Apache or iptables to just refuse connections to certain countries?

You can block traffic at both Apache or iptables level. I recommend iptables to save some resources. First, you need to get list of netblocks for each country. Simply [visit](#) ^[3] this page and download IP block files are provided in CIDR format. Use the following shell script:



[2]



[1]



WARNING! People from other countries may use proxy server or think of spoofing their IP address. In such case, this may not work and it will only protect your box from automated scans or spam.

```
#!/bin/bash
### Block all traffic from AFGHANISTAN (af) and CHINA (CN). Use ISO code ###
ISO="af cn"

### Set PATH ###
IPT=/sbin/iptables
WGET=/usr/bin/wget
EGREP=/bin/egrep

### No editing below ###
SPAMLIST="countrydrop"
ZONEROOT="/root/iptables"
DLROOT="http://www.ipdeny.com/ipblocks/data/countries"

cleanOldRules() {
$IPT -F
$IPT -X
$IPT -t nat -F
$IPT -t nat -X
$IPT -t mangle -F
$IPT -t mangle -X
$IPT -P INPUT ACCEPT
$IPT -P OUTPUT ACCEPT
$IPT -P FORWARD ACCEPT
}

# create a dir
[ ! -d $ZONEROOT ] && /bin/mkdir -p $ZONEROOT

# clean old rules
cleanOldRules

# create a new iptables list
$IPT -N $SPAMLIST

for c in $ISO
do
# local zone file
tDB=$ZONEROOT/$c.zone

# get fresh zone file
$WGET -O $tDB $DLROOT/$c.zone

# country specific log message
```

```

SPAMDROPMMSG="$c Country Drop"

# get
BADIPS=$(egrep -v "^#|^$" $tDB)
for ipblock in $BADIPS
do
    $IPT -A $SPAMLIST -s $ipblock -j LOG --log-prefix "$SPAMDROPMMSG"
    $IPT -A $SPAMLIST -s $ipblock -j DROP
done
done

# Drop everything
$IPT -I INPUT -j $SPAMLIST
$IPT -I OUTPUT -j $SPAMLIST
$IPT -I FORWARD -j $SPAMLIST

# call your other iptable script
# /path/to/other/iptables.sh

exit 0

```

Save above script as root user and customize ISO variable to point out country name using ISO country names. Once done install the script as follows using [crontab](#) ^[4]:

```
@weekly /path/to/country.block.iptables.sh
```

To start blocking immediately type:

```
# /path/to/country.block.iptables.sh
```

And you are done with blocking the whole country from your server.

iptables geoip patch

Another, alternative to above shell script is to use geoip iptables patch. This is not standard iptables modules. You need to download patch and compile Linux kernel.

- Grab geoip patch from the [official website](#) ^[5].
- Download and install Linux kernel and iptables source code.
- Grab and install tool called [patch-o-matic](#) ^[6] (required for geoip modules).
- Finally, grab GEO IP database from [MaxMind](#) ^[7].

The details of kernel compile and iptables patching are beyond the scope of this FAQ. This is left as an exercise to readers.

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our [daily email](#) newsletter or [weekly newsletter](#) to make sure you don't miss a single tip/tricks. Alternatively, subscribe via [RSS/XML](#) feed.

Article printed from Frequently Asked Questions About Linux / UNIX: <http://www.cyberciti.biz/faq/>

URL to article: <http://www.cyberciti.biz/faq/block-entier-country-using-iptables/>

URLs in this post:

[1] Image: <http://www.cyberciti.biz/faq/category/iptables/>

[2] Image: <http://www.cyberciti.biz/faq/category/apache/>

[3] visit: <http://www.ipdeny.com/ipblocks/>

[4] crontab: <http://www.cyberciti.biz/faq/how-do-i-add-jobs-to-cron-under-linux-or-unix-oses/>

[5] official website: <http://people.netfilter.org/peejix/patchlets/>

[6] patch-o-matic: <http://ftp.netfilter.org/pub/patch-o-matic-ng/snapshot/>

[7] MaxMind: <http://www.maxmind.com/>

Copyright © 2006-2010 [nixCraft](#). All rights reserved. This print / pdf version is for personal non-commercial use only. More details <http://www.cyberciti.biz/tips/copyright>.