

Filter by country (Geoip)

- An average email server **rejects between 30-90%** of emails as spam.
- We can filter traffic **based on the country** the packet is coming from or destined to.
- iptables uses **xt_geoip** which consists of an extension named **xtable_addon** and GeoIP database to perform country specific filtering.
- xt_geoip **doesn't belong** to the standard netfilter/iptables framework. It should be installed.
- The country is specified using the **ISO 3166** code:
https://en.wikipedia.org/wiki/ISO_3166-1

Filter by country (Geoip) - installation & config

1. Install xtables-addons and dependencies

Ubuntu: `sudo apt-get update && sudo apt-get install xtables-addons-common libtext-csv-xs-perl pkg-config iptables-dev`

CentOS: `yum update && yum install gcc-c++ make automake kernel-devel`uname -r` wget unzip iptables-devel perl-Text-CSV_XS`

2. Download GeoIP list (from MaxMind) as a CSV file

From a temp directory (ex: /tmp) run: `sudo /usr/lib/xtables-addons/xt_geoip_dl`

3. Create a folder for converted files and import them into xtables

`sudo mkdir /usr/share/xt_geoip`

`sudo /usr/lib/xtables-addons/xt_geoip_build -D /usr/share/xt_geoip *.csv`

4. Test it!

`iptables -m geoip --help`