Allow or block whole countries

Install xtables-addons

You can install the xtables-addons module using various methods, feel free to use the installation method that works best for you.

* Install usingapt-get.
* sudo apt-get install xtables-addons-common
* Install using module-assistant.
* sudo apt-get install module-assistant xtables-addons-source
* sudo module-assistant --verbose --text-mode auto-install xtables-addons
* Install from source.
* sudo apt-get install git bc libncurses5-dev libtext-csv-xs-perl autoconf automake libtool xutils-dev iptables-dev
* git clone git://git.code.sf.net/p/xtables-addons/xtables-addons
* cd xtables-addons
* ./autogen.sh
* ./configure
* make
* sudo make install

Build a "countries" database.

sudo apt-get install libtext-csv-xs-perl unzip

sudo mkdir /usr/share/xt\_geoip

sudo /usr/lib/xtables-addons/xt\_geoip\_dl

sudo /usr/lib/xtables-addons/xt\_geoip\_build -D /usr/share/xt\_geoip \*.csv

sudo rm GeoIPCountryCSV.zip GeoIPCountryWhois.csv GeoIPv6.csv

Reboot your system.

sudo reboot

After xtables-addons has been successfully installed, after the first reboot, run depmod otherwise country blocking will not work properly (this is only required for the first time).

sudo depmod

Create a script at /etc/cron.monthly/geoip-updater to update the geoip database monthly.

#!/usr/bin/env bash

# this script is intended to run with sudo privileges

echo 'Removing old database---------------------------------------------------'

rm -rf /usr/share/xt\_geoip/\*

mkdir -p /usr/share/xt\_geoip

echo 'Downloading country databases-------------------------------------------'

mkdir /tmp/geoip-updater

cd /tmp/geoip-updater

/usr/lib/xtables-addons/xt\_geoip\_dl

echo 'Building geoip database-------------------------------------------------'

/usr/lib/xtables-addons/xt\_geoip\_build -D /usr/share/xt\_geoip \*.csv

echo 'Removing temporary files------------------------------------------------'

cd /tmp

rm -rf /tmp/geoip-updater

Make /etc/cron.monthly/geoip-updater executable.

sudo chmod +x /etc/cron.monthly/geoip-updater

Example rules

\_Note: If you are receiving an iptables: No chain/target/match by that name error when trying to apply a geoip rule, it's possible that xtables-addons has not been installed correctly. Try another installation method.

Block all incoming packets from China, Hong Kong, Russia and Korea.

sudo iptables -A INPUT -m geoip --src-cc CN,HK,RU,KR -j DROP

Allow incoming packets on port 80 from everywhere except the countries above.

sudo iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT

Allow incoming packets on the ens3 interface on port 22 only from Peru (feel free to choose the country code you want to accept packets from, for example, US for United States).

sudo iptables -A INPUT -i ens3 -p tcp -m tcp --dport 22 -m geoip --src-cc PE -j ACCEPT

Allow incoming packets on port 443 only from Peru.

sudo iptables -A INPUT -p tcp -m tcp --dport 443 -m geoip --src-cc PE -j ACCEPT