How to block specific countries from accessing your server

Applies to VoipNow 3.X.X and upper versions!

An increased number of VoIP attacks (mostly brute-force) coming from specific countries usually leads to excessive resource utilization. If successful, such attacks might eventually lead to fraud calls. One way to avoid this situation is by blocking specific countries - one or more.

Before starting

It is assumed that you are using a CentOS 7 server already having *iptables* and *ipset* installed. Run the following command in order to double check the availability of the packages:

yum list ipset iptables ipset-service iptables-services
In case all are listed under "Installed Packages" section, you can proceed forward. Otherwise, just install the missing packages.
yum install ipset iptables ipset iptables ipset-service iptables-services

Step-by-step guide

1. Download the script.

   wget -O blockcountry.pl https://raw.githubusercontent.com/4psa/voipnowtoolbox/master/blockcountry.pl

2. Install the required perl libraries using the following command. As one of them is available only on EPEL, the EPEL Repository must be added first:

   yum install epel-release perl-libwww-perl perl-Locale-SubCountry

3. Edit the *blockcountry.pl* script and specify which countries you want to block. The list of countries is available here.

   ```
   my @countries = (
           "PS",
           "SA",
           "TR",
           );
   ```

4. Run the *blockcountry.pl* script:

   perl blockcountry.pl

   The default policy is set to reject. The iptables rules for the above example look like this:

   ```
   Chain INPUT (policy ACCEPT)
   target     prot opt source               destination
   REJECT     all  --  0.0.0.0/0            0.0.0.0/0            match-set Turkey src reject-with icmp-host-
   unreachable
   REJECT     all  --  0.0.0.0/0            0.0.0.0/0            match-set Saudi_Arabia src reject-with
   icmp-host-unreachable
   REJECT     all  --  0.0.0.0/0            0.0.0.0/0            match-set Palestinian_Territory_Occupied
   src reject-with icmp-host-unreachable
   ```

   If you want to add the iptables rules with ACCEPT or DROP instead of reject, you can call the script with *-p* parameter.

   perl blockcountry.pl -p drop
   It will add the iptables rule as follows:

   ```
   Chain INPUT (policy ACCEPT)
   target     prot opt source               destination
   DROP           all  --  0.0.0.0/0            0.0.0.0/0            match-set Turkey src
   DROP           all  --  0.0.0.0/0            0.0.0.0/0            match-set Saudi_Arabia src
   DROP           all  --  0.0.0.0/0            0.0.0.0/0            match-set
   Palestinian_Territory_Occupied src
   ```

   Daily refresh of the IP sets can be done via a cronjob like the one below:

```
* 1 * * * /usr/bin/perl /<path_to_the_script>/blockcountry.pl -r > /dev/null 2>&1
```

Replace <*path_to_the_script*> with the actual path toward the *blockcountry.pl* script.

If you need to flush the existing rules and destroy all the IP sets available, use the parameter *-f* like this:

perl blockcountry.pl -f
Just answer Yes or Y and all the rules and sets will be removed.

5. To preserve the rules during reboots, run the following command:

   service iptables save && service ipset save

Make sure you do not mix up the countries, otherwise you might get yourself blocked.

To avoid such issues, it is recommended to start with a cronjob that will remove the rules. If no issues arise, the cronjob can be removed.

Related articles

- Primary and secondary server setup for 4PSA DNS Manager
- How to block specific countries from accessing your server
- How to find out how many DNS queries are being made
- How to dump zones remotely from a Plesk Windows server
- How to debug Asterisk and Kamailio