endian

Secure everyThing
www.endian.com

HOW-TO: Enable and Set GEO-IP Filter via CLI -Preview Feature

Marco Pomalo

Document Revision: 13

Last Modification: 05/07/2021

Exported on: 05/17/2021

Exported by: Luis Aigner

Document URL: https://confluence.endian.com/display/~m.pomalo/HOW-TO%3A+Enable+and+Set+GEO-IP+Filter+via+CLI+-Preview+Feature

Table of contents

HOW-TO: Enable and Set GEO-IP Filter via CLI -Preview Feature

Document Version: 1.0

Applies to EOS: 5 and EOS 6

Applies to platform: all

This lesson shows how to set a Geo-IP firewall filter from the Command Line Interface (CLI). Since this is a preview feature, it is not yet implemented in the GUI, which will be updated in the next EOS Release.

Requirements

This how-to needs an updated appliance to EOS 5.2.6 or EOS 6.1.3

What is a Geo-IP

The network communication on the Internet is based on IP addresses, that allow a unique identification of connected devices. These addresses are assigned in blocks to countries worldwide, avoiding duplicates. Each country manages the own assigned address blocks.

For example, considering only IPV4 addresses to keep it simple, country A could have been assigned among others a block from 59.32.0.0 to 59.83.255.255 , and country B could have been assigned a block from 5.187.64.0 to 5.187.95.255 .

By reversing this concept, we can easily determine the country from a public IP address. In other words, a Geo-IP is a plain IP address related to a specific geographic location e.g. represented by a country.

Why do we need a Geo-IP filter

The recent cyber attack on Microsoft Exchange servers worldwide, and other cyberattacks, proved that the origin of most of this criminal behaviour comes from very specific countries, therefore protecting the own infrastructure by filtering network traffic from or to those countries is nowadays a must.

How to proceed

1. Login the appliance with root user using SSH. It can be done in two ways:
   a. directly from the Endian Network as described in the first part of this guide: https://help.endian.com/hc/it/articles/360024569533-How-to-use-Endian-Network
   b. or from a computer using Putty (Windows) or Terminal (MAC/Linux).
2. You should get a screen like this:

Root user successful login

```
  eeee      _nn_        dd   ii    _aa       _nn_
 ee""ee    _n""n_       dd   -     a"a_     _n""n_
 ee  ee    nn  nn       dd            a     nn  nn
 ee  ee    nn  nn    _dddd   ii    _aaa     nn  nn
 ee  ee    nn  nn   _d""dd   ii   _a""aa    nn  nn
 ee__ee    nn  nn   dd  dd   ii   aa  aa    nn  nn
 eeee"     nn  nn   dd  dd   ii   aa  aa    nn  nn
 ee"       nn  nn   dd  dd   ii   aa  aa    nn  nn
 ee        nn  nn   dd  dd   ii   aa  aa    nn  nn
  ee       nn  nn   dd  dd   ii   aa  aa    nn  nn
   ee      nn  nn    ddddd   ii    aaaaa    nn  nn
    -"     -"  "'     -'-"   "'     -'-"    "'  -"

 ||  ||  ||  ||  ||  ||  ||||||||||||||||||||

          Endian Firewall Enterprise

WARNING!   -  CHANGES TO SYSTEM FILES MAY AFFECT
YOUR  WARRANTY  AND DISCHARGE  ENDIAN  FROM  ANY
FURTHER  OBLIGATION  TO  PROVIDE  CUSTOMER  WITH
WARRANTY SERVICES OR SUPPORT HEREUNDER!

Have fun with your Endian Firewall!

root@efw-mini25:~ #
```

3. You need to create/edit two files. Please skip this step if you already know how to create/edit files, otherwise proceed as described in this guide: https://help.endian.com/hc/it/articles/218146618-Endian-s-startup-scripts-with-inithooks
4. Create/edit file: ***/var/efw/inithooks/start.local*** by typing following command: (we use **nano** editor in this guide)

```
root@efw-mini25:~ # nano /var/efw/inithooks/start.local
```

   a. Add '"/var/efw/inithooks/rc.firewall.local start" line to the file, which triggers the execution of additional firewall rules.

b. The content of the file should be similar to this:

File: /var/efw/inithooks/start.local

```
#!/bin/bash
# Add your code here
/var/efw/inithooks/rc.firewall.local start
exit 0
```

5. Now create/edit file: ***/var/efw/inithooks/rc.firewall.local*** by typing following command: (we use **nano** editor in this guide)

```
root@efw-mini25:~ # nano /var/efw/inithooks/rc.firewall.local
```

a. The comments in the file example below explain what every line does.
   i. The commands in section "start" clear the rules, and block the traffic from and to China (CN), Russia (RU), and North Korea (KP). At the end of this guide you will find the country codes you may need to set.
   ii. The commands in section "stop" clear the rules.
   iii. The commands in section "reload" do the same as those in the "start" section.

b. The content of the file should be similar to this:

File: /var/efw/inithooks/rc.firewall.local

```
#!/bin/bash
# See how we were called.
case "$1" in
start)
## add your 'start' rules here
##
## Following rule clears the chain
iptables -F CUSTOMFORWARD
##
## Following rule blocks incoming traffic FROM selected countries
iptables -I CUSTOMINPUT -m geoip --source-country=RU,CN,KP -j DROP
##
## Following rule blocks forwarded traffic TO selected countries
iptables -I CUSTOMFORWARD -m geoip --destination-country RU,CN,KP -j DROP
;;
stop)
## add your 'stop' rules here
## Following rule clears the chain
iptables -F CUSTOMFORWARD
;;
reload)
## add your 'reload' rules here
##
## Following rule clears the chain
iptables -F CUSTOMFORWARD
##
## Following rule blocks incoming traffic FROM selected countries
iptables -I CUSTOMINPUT -m geoip --source-country=RU,CN.KP -j DROP
##
## Following rule blocks forwarded traffic TO selected countries
iptables -I CUSTOMFORWARD -m geoip --destination-country RU,CN,KP -j DROP
;;
*)
echo "Usage: $0 {start|reload|stop}"
esac
```

IMPORTANT!! Please do not forget to set the correct permissions to the files by executing the following commands:

```
root@efw-mini25:~ # chmod 755 /var/efw/inithooks/start.local
root@efw-mini25:~ # chmod 755 /var/efw/inithooks/rc.firewall.local
```

Manually Enable/Disable Firewall Filter from CLI

Now you can test if everything is correct by enabling or disabling the new firewall filter. You will get CLI feedback only in case of errors.

ENABLE/DISABLE firewall filter

```
root@efw-mini25:~ # /var/efw/inithooks/rc.firewall.local start
root@efw-mini25:~ # /var/efw/inithooks/rc.firewall.local stop
```

Additional Information

Here you find the ISO 3166 country codes which can be used to filter country specific network traffic.

Geo-IP ISO 3166 Country Codes

```
A1,"Anonymous Proxy"
A2,"Satellite Provider"
O1,"Other Country"
AD,"Andorra"
AE,"United Arab Emirates"
AF,"Afghanistan"
AG,"Antigua and Barbuda"
AI,"Anguilla"
AL,"Albania"
AM,"Armenia"
AO,"Angola"
AP,"Asia/Pacific Region"
AQ,"Antarctica"
AR,"Argentina"
AS,"American Samoa"
AT,"Austria"
AU,"Australia"
AW,"Aruba"
AX,"Aland Islands"
AZ,"Azerbaijan"
BA,"Bosnia and Herzegovina"
BB,"Barbados"
BD,"Bangladesh"
BE,"Belgium"
BF,"Burkina Faso"
```

```
BG,"Bulgaria"
BH,"Bahrain"
BI,"Burundi"
BJ,"Benin"
BL,"Saint Barthelemy"
BM,"Bermuda"
BN,"Brunei Darussalam"
BO,"Bolivia"
BQ,"Bonaire, Saint Eustatius and Saba"
BR,"Brazil"
BS,"Bahamas"
BT,"Bhutan"
BV,"Bouvet Island"
BW,"Botswana"
BY,"Belarus"
BZ,"Belize"
CA,"Canada"
CC,"Cocos (Keeling) Islands"
CD,"Congo, The Democratic Republic of the"
CF,"Central African Republic"
CG,"Congo"
CH,"Switzerland"
CI,"Cote d'Ivoire"
CK,"Cook Islands"
CL,"Chile"
CM,"Cameroon"
CN,"China"
CO,"Colombia"
CR,"Costa Rica"
CU,"Cuba"
CV,"Cape Verde"
CW,"Curacao"
CX,"Christmas Island"
CY,"Cyprus"
CZ,"Czech Republic"
DE,"Germany"
DJ,"Djibouti"
DK,"Denmark"
DM,"Dominica"
DO,"Dominican Republic"
DZ,"Algeria"
EC,"Ecuador"
EE,"Estonia"
EG,"Egypt"
EH,"Western Sahara"
ER,"Eritrea"
ES,"Spain"
ET,"Ethiopia"
EU,"Europe"
FI,"Finland"
FJ,"Fiji"
```

```
FK,"Falkland Islands (Malvinas)"
FM,"Micronesia, Federated States of"
FO,"Faroe Islands"
FR,"France"
GA,"Gabon"
GB,"United Kingdom"
GD,"Grenada"
GE,"Georgia"
GF,"French Guiana"
GG,"Guernsey"
GH,"Ghana"
GI,"Gibraltar"
GL,"Greenland"
GM,"Gambia"
GN,"Guinea"
GP,"Guadeloupe"
GQ,"Equatorial Guinea"
GR,"Greece"
GS,"South Georgia and the South Sandwich Islands"
GT,"Guatemala"
GU,"Guam"
GW,"Guinea-Bissau"
GY,"Guyana"
HK,"Hong Kong"
HM,"Heard Island and McDonald Islands"
HN,"Honduras"
HR,"Croatia"
HT,"Haiti"
HU,"Hungary"
ID,"Indonesia"
IE,"Ireland"
IL,"Israel"
IM,"Isle of Man"
IN,"India"
IO,"British Indian Ocean Territory"
IQ,"Iraq"
IR,"Iran, Islamic Republic of"
IS,"Iceland"
IT,"Italy"
JE,"Jersey"
JM,"Jamaica"
JO,"Jordan"
JP,"Japan"
KE,"Kenya"
KG,"Kyrgyzstan"
KH,"Cambodia"
KI,"Kiribati"
KM,"Comoros"
KN,"Saint Kitts and Nevis"
KP,"Korea, Democratic People's Republic of"
KR,"Korea, Republic of"
```

```
KW,"Kuwait"
KY,"Cayman Islands"
KZ,"Kazakhstan"
LA,"Lao People's Democratic Republic"
LB,"Lebanon"
LC,"Saint Lucia"
LI,"Liechtenstein"
LK,"Sri Lanka"
LR,"Liberia"
LS,"Lesotho"
LT,"Lithuania"
LU,"Luxembourg"
LV,"Latvia"
LY,"Libyan Arab Jamahiriya"
MA,"Morocco"
MC,"Monaco"
MD,"Moldova, Republic of"
ME,"Montenegro"
MF,"Saint Martin"
MG,"Madagascar"
MH,"Marshall Islands"
MK,"Macedonia"
ML,"Mali"
MM,"Myanmar"
MN,"Mongolia"
MO,"Macao"
MP,"Northern Mariana Islands"
MQ,"Martinique"
MR,"Mauritania"
MS,"Montserrat"
MT,"Malta"
MU,"Mauritius"
MV,"Maldives"
MW,"Malawi"
MX,"Mexico"
MY,"Malaysia"
MZ,"Mozambique"
NA,"Namibia"
NC,"New Caledonia"
NE,"Niger"
NF,"Norfolk Island"
NG,"Nigeria"
NI,"Nicaragua"
NL,"Netherlands"
NO,"Norway"
NP,"Nepal"
NR,"Nauru"
NU,"Niue"
NZ,"New Zealand"
OM,"Oman"
PA,"Panama"
```

```
PE,"Peru"
PF,"French Polynesia"
PG,"Papua New Guinea"
PH,"Philippines"
PK,"Pakistan"
PL,"Poland"
PM,"Saint Pierre and Miquelon"
PN,"Pitcairn"
PR,"Puerto Rico"
PS,"Palestinian Territory"
PT,"Portugal"
PW,"Palau"
PY,"Paraguay"
QA,"Qatar"
RE,"Reunion"
RO,"Romania"
RS,"Serbia"
RU,"Russian Federation"
RW,"Rwanda"
SA,"Saudi Arabia"
SB,"Solomon Islands"
SC,"Seychelles"
SD,"Sudan"
SE,"Sweden"
SG,"Singapore"
SH,"Saint Helena"
SI,"Slovenia"
SJ,"Svalbard and Jan Mayen"
SK,"Slovakia"
SL,"Sierra Leone"
SM,"San Marino"
SN,"Senegal"
SO,"Somalia"
SR,"Suriname"
SS,"South Sudan"
ST,"Sao Tome and Principe"
SV,"El Salvador"
SX,"Sint Maarten"
SY,"Syrian Arab Republic"
SZ,"Swaziland"
TC,"Turks and Caicos Islands"
TD,"Chad"
TF,"French Southern Territories"
TG,"Togo"
TH,"Thailand"
TJ,"Tajikistan"
TK,"Tokelau"
TL,"Timor-Leste"
TM,"Turkmenistan"
TN,"Tunisia"
TO,"Tonga"
```

```
TR,"Turkey"
TT,"Trinidad and Tobago"
TV,"Tuvalu"
TW,"Taiwan"
TZ,"Tanzania, United Republic of"
UA,"Ukraine"
UG,"Uganda"
UM,"United States Minor Outlying Islands"
US,"United States"
UY,"Uruguay"
UZ,"Uzbekistan"
VA,"Holy See (Vatican City State)"
VC,"Saint Vincent and the Grenadines"
VE,"Venezuela"
VG,"Virgin Islands, British"
VI,"Virgin Islands, U.S."
VN,"Vietnam"
VU,"Vanuatu"
WF,"Wallis and Futuna"
WS,"Samoa"
YE,"Yemen"
YT,"Mayotte"
ZA,"South Africa"
ZM,"Zambia"
ZW,"Zimbabwe"
```