Разрешение доступа по гео с iptables

Устанавливаем необходимые пакеты:

```
apt-get -y install iptables-persistent
apt-get -y install ipset
```

Для постоянности работы ipset необходимо создать службу `/etc/systemd/system/ipset-persistent.service`:

```
[Unit]
Description=ipset persistent configuration
Before=network.target

# ipset sets should be loaded before iptables
# Because creating iptables rules with names of non-existent sets is not possible
Before=netfilter-persistent.service
Before=ufw.service

ConditionFileNotEmpty=/etc/iptables/ipset

[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/sbin/ipset restore -exist -file /etc/iptables/ipset
# Uncomment to save changed sets on reboot
# ExecStop=/sbin/ipset save -file /etc/iptables/ipset
ExecStop=/sbin/ipset flush
ExecStopPost=/sbin/ipset destroy

[Install]
WantedBy=multi-user.target
RequiredBy=netfilter-persistent.service
RequiredBy=ufw.service
```

Включаем нашу службу:

```
systemctl daemon-reload
systemctl enable ipset-persistent.service
systemctl restart ipset-persistent.service
```

Создаем новую зону содержащую российские подсети:

```
ipset create "RU_zone" hash:net
for IP in $(wget -O - https://www.ipdeny.com/ipblocks/data/countries/ru.zone); do ipset add "RU_zone" $IP; done
```

Проверяем, что добавились подсети в зону:

```
ipset -L RU_zone | less
```

Для персистентности подсетей сохраняем и подгружаем их из файла:

```
ipset save > /etc/iptables/ipset
ipset restore < /etc/iptables/ipset
```

Сохраняем текущие правила iptables:

```
iptables-save > /root/rules.v4
```

Добавляем разрешение в нужном месте (определите его самостоятельно) доступа по гео в сохраненном файле /root/rules.v4:

```
-A INPUT -p tcp -m set --match-set RU_zone src -m tcp --dport 22000 -j ACCEPT
```

Для персистентности правил сохраняем их:

```
cp /root/rules.v4 /etc/iptables/rules.v4
```

Применение новых правил iptables:

```
iptables-restore < /etc/iptables/rules.v4
```

> Полезная утилита для мониторинга работы iptables - **iptstate**

Revision #1
Created 28 May 2024 13:15:18 by Boris Rzr
Updated 28 May 2024 13:27:16 by Boris Rzr