

# Защита

- Филтрация по странам
- RDP сервер за NAT

# Фильтрация по странам

Список стран:

“ <http://www.iwik.org/ipcountry/>

Поменять CN на необходимую страну, либо добавить дополнительные строки с нужными странами:

```
/system scheduler
add disabled=no interval=1d name=CN on-event=backup policy=\
  ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon \
  start-date=jan/10/2020 start-time=00:00:01

/system script
add dont-require-permissions=no name=CN owner=admin policy=\
  ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon source="\
\n/tool fetch url=http://www.iwik.org/ipcountry/mikrotik/CN;\r\
\n/import file-name=CN;\r\
\n/file remove CN;\r\
\n"

/ip firewall raw
add chain=prerouting action=drop in-interface-list=WAN log=no log-prefix="" src-address-list=CN
```

# RDP сервер за NAT

Если сервер на другом порту, сменить 3389 на нужный

```
/ip firewall filter add action=reject chain=forward reject-with=icmp-network-unreachable src-address-list="Blocked bruteforcers"

/ip firewall filter add action=add-src-to-address-list address-list="Blocked bruteforcers" address-list-timeout=60m chain=forward connection-state=new in-interface=EXT dst-port=3389 log=yes log-prefix="RDP BRUTEFORCE - " protocol=tcp src-address-list=rdp_bruteforce3

/ip firewall filter add action=add-src-to-address-list address-list=rdp_bruteforce3 address-list-timeout=15m chain=forward connection-state=new in-interface=EXT dst-port=3389 protocol=tcp src-address-list=rdp_bruteforce2

/ip firewall filter add action=add-src-to-address-list address-list=rdp_bruteforce2 address-list-timeout=15m chain=forward connection-state=new in-interface=EXT dst-port=3389 protocol=tcp src-address-list=rdp_bruteforce1

/ip firewall filter add action=add-src-to-address-list address-list=rdp_bruteforce1 address-list-timeout=15m chain=forward connection-state=new in-interface=EXT dst-port=3389 protocol=tcp
```