Mikrotik

- Защита
  - Фильтрация по странам
  - RDP сервер за NAT
- Общее
  - Балансировка серверов
  - Блокировка обновлений Microsoft
  - Включение FastTrack
  - Использование DNS сервера для домена
  - Исправление проблем с RDP
  - Ставим CHR на VDS
  - Транзит одинаковых сетей
- Backup
  - Вариант 1
  - Вариант 2

Защита

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
```

Защита

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
```

Общее

Общее

Балансировка серверов

123.123.123.123 - внешний адрес

80 - порт сервиса для балансировки

192.168.0.1 и 192.168.0.2 - внутренние сервера

```
add action=dst-nat chain=dstnat dst-address=123.123.123.123 dst-port=80 per-connection-classifier=both-addresses-and-ports:2/0 protocol=tcp to-addresses=192.168.0.1
add action=dst-nat chain=dstnat dst-address=123.123.123.123 dst-port=80 per-connection-classifier=both-addresses-and-ports:2/1 protocol=tcp to-addresses=192.168.0.2
```

Общее

Блокировка обновлений Microsoft

Вариант 1

```
/ip firewall raw
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=windowsupdate.microsoft.com
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=*.windowsupdate.microsoft.com
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=download.microsoft.com
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=test.stats.update.microsoft.com
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=ntservicepack.microsoft.com
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=stats.microsoft.com
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=wustat.windows.com
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=windowsupdate.com
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=download.windowsupdate.com
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=*.download.windowsupdate.com
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=update.microsoft.com
add action=drop chain=prerouting comment="WSUS" protocol=tcp tls-host=*.update.microsoft.com

/system scheduler
add name="WSUS_on" on-event="/ip firewall raw disable [find comment=\"WSUS\"]" start-date=Aug/12/2021
start-time=00:01:00 interval=7d comment="" disabled=no
add name="WSUS_off" on-event="/ip firewall raw enable [find comment=\"WSUS\"]" start-date=Aug/12/2021
start-time=00:08:00 interval=7d comment="" disabled=no
```

Вариант 2

```
/ip firewall raw
add action=drop chain=prerouting comment="WSUS" content=windowsupdate.microsoft.com
add action=drop chain=prerouting comment="WSUS" content=.windowsupdate.microsoft.com
add action=drop chain=prerouting comment="WSUS" content=download.microsoft.com
add action=drop chain=prerouting comment="WSUS" content=test.stats.update.microsoft.com
add action=drop chain=prerouting comment="WSUS" content=ntservicepack.microsoft.com
add action=drop chain=prerouting comment="WSUS" content=stats.microsoft.com
```

```
add action=drop chain=prerouting comment="WSUS" content=wustat.windows.com
add action=drop chain=prerouting comment="WSUS" content=windowsupdate.com
add action=drop chain=prerouting comment="WSUS" content=download.windowsupdate.com
add action=drop chain=prerouting comment="WSUS" content=.download.windowsupdate.com
add action=drop chain=prerouting comment="WSUS" content=update.microsoft.com
add action=drop chain=prerouting comment="WSUS" content=.update.microsoft.com

/system scheduler
add name="WSUS_on" on-event="/ip firewall raw disable [find comment=\"WSUS\"]" start-date=Aug/12/2021
start-time=00:01:00 interval=7d comment="" disabled=no
add name="WSUS_off" on-event="/ip firewall raw enable [find comment=\"WSUS\"]" start-date=Aug/12/2021
start-time=00:08:00 interval=7d comment="" disabled=no
```

Общее

Включение FastTrack

```
/ip firewall filter add chain=forward action=fasttrack-connection connection-state=established,related
/ip firewall filter add chain=forward action=accept connection-state=established,related
```

Общее

Использование DNS сервера для домена

Сменить <123.123.123.123> и <.*mynetname\\.net> на нужные

```
/ip dns static add forward-to=<123.123.123.123> regexp="<.*mynetname\\.net>" ttl=10m type=FWD
```

Общее

Исправление проблем с RDP

При использовании RDP соединений внутри VPN или туннелей иногда возникают проблемы с отвалом сессий. Причина в том, что RDP после подключения начинает открывать UDP сессии, помимо уже установленной TCP.

Решается блокировкой RDP трафика по UDP:

```
/ip firewall raw add chain=prerouting action=drop dst-port=3389 protocol=udp
```

Общее

Ставим CHR на VDS

Ubuntu

- Разворачиваем на хостинге Linux дистрибутив
- Логинимся на сервер и получаем права суперпользователя:

```
sudo -i
```

- Обновляем пакетную базу и устанавливаем необходимые пакеты:

```
apt update && apt -y install unzip wget
```

- Скачиваем raw образ системы (актуальные ссылки смотрим на сайте в разделе загрузок):

```
wget https://download.mikrotik.com/routeros/6.47.4/chr-6.47.4.img.zip
```

- Распаковываем образ:

```
unzip chr-6.47.4.img.zip
```

- Включаем сочетания SysRq:

```
echo "1" > /proc/sys/kernel/sysrq
```

- Переподключаем все файловые системы в режиме чтения:

```
echo u > /proc/sysrq-trigger
```

- Находим название системного диска:

```
lsblk
```

- Записываем на него образ:

```
dd if=chr-6.47.4.img of=/dev/vda bs=4M oflag=sync
```

- Перезагружаем виртуальную машину:

```
echo "b" > /proc/sysrq-trigger
```

- После перезапуска, вместо линукс системы, будет запущен Mikrotik CHR, развернутый на весь объем жесткого диска

CentOS

- Разворачиваем на хостинге Linux дистрибутив
- Логинимся на сервер и получаем права суперпользователя:

```
sudo -i
```

- Обновляем пакетную базу и устанавливаем необходимые пакеты:

```
yum install wget unzip
```

- Монтируем tmpfs в /tmp:

```
mount -t tmpfs tmpfs /tmp
```

- Переходим в директорию tmp и скачиваем raw образ системы (актуальные ссылки смотрим на сайте в разделе загрузок):

```
cd /tmp && wget https://download.mikrotik.com/routeros/6.47.4/chr-6.47.4.img.zip
```

- Распаковываем образ:

```
unzip chr-6.47.4.img.zip
```

- Включаем сочетания SysRq:

```
echo "1" > /proc/sys/kernel/sysrq
```

- Находим название системного диска:

```
lsblk
```

- Записываем на него образ:

```
dd if=chr-6.47.4.img of=/dev/vda bs=4M oflag=sync
```

- Перезагружаем виртуальную машину:

```
echo "b" > /proc/sysrq-trigger
```

- После перезапуска, вместо линукс системы, будет запущен Mikrotik CHR, развернутый на весь объем жесткого диска

Общее

Транзит одинаковых сетей

-> Interface

Добавляем новый туннель до точки. В поле name указать тип туннеля, подключаемую компанию и удаленную точку (например ipip-kolobok-gw). Keepalive убрать.

-> IP -> Addresses

Добавляем новый адрес для туннеля. Адрес должен быть из свободного пула подсети 100.64.0.0/10 с маской 24 (например 100.80.23.1/24).

-> IP -> Firewall -> Mangle

Добавляем правило prerouting и dst. address выставляем адрес фейковой сети из свободного пула 10.0.0.0/8 (например 10.51.0.0/24).

В action выставляем mark routing с new routing mark из названия туннеля без указания его типа (например kolobok-gw).

-> IP -> Firewall -> NAT

Добавляем правило srcnat с src. address реальной сети удаленной стороны (например 192.168.0.0/24), out. interface ставим название туннеля (например ipip-kolobok-gw), в action ставим netmap на фэйковую сеть (например 10.51.0.0/24).

Добавляем правило dstnat с dst. address фэйковой сети (например 10.51.0.0/24), в action ставим netmap на реальную сеть удаленной стороны (например 192.168.0.0/24).

-> IP -> Routes

Добавляем правило dst. address фэйковой сети (например 10.51.0.0/24), в gateway название туннеля (например ipip-kolobok-gw) и distance 20.

Добавляем правило dst. address реальной сети удаленной стороны (например 192.168.0.0/24), в gateway название туннеля (например ipip-kolobok-gw), distance 30 и routing mark из названия туннеля без указания его типа (например kolobok-gw).

Backup

Вариант 1

Поменять <SERVER>, <USER> и <PASSWORD>на свои значения FTP сервера

```
/log info "backup starting";
:local CurrentTime [/system clock get time];
:local CurrentDate [/system clock get date];
:local Hour [:tostr [:pick $CurrentTime 0 2]];
:local Min [:tostr [:pick $CurrentTime 3 5]];
:local Day [:tostr [:pick $CurrentDate 4 6]];
:local Month [:tostr [:pick $CurrentDate 0 3]];
:local Year [:tostr [:pick $CurrentDate 7 [:len $CurrentDate]]];
:global name=backupfile value=([/system identity get name] ."__$Day_$Month_$Year__$Hour_$Min.backup")
:global name=scriptfile value=([/system identity get name] ."__$Day_$Month_$Year__$Hour_$Min.rsc")
/system backup save name=$backupfile;
/export verbose file=$scriptfile;
:delay 10s
/tool fetch address=<SERVER> src-path=$backupfile user=<USER> mode=ftp password=<PASSWORD> dst-path="backup/$backupfile" upload=yes;
/tool fetch address=<SERVER> src-path=$scriptfile user=<USER> mode=ftp password=<PASSWORD> dst-path="backup/$scriptfile" upload=yes;
:delay 20s
/file remove $backupfile;
/file remove $scriptfile;
/log info "backup finished";
```

Вариант 2

Поменять <SERVER>, <USER> и <PASSWORD>на свои значения FTP сервера

```
/system scheduler
add disabled=no interval=5d name=backup 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=backup owner=su policy=\
  ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon source="/\
  log info \"backup starting\";\r\
  \n:local CurrentTime [/system clock get time];\r\
  \n:local CurrentDate [/system clock get date];\r\
  \n:local Hour [:tostr [:pick \$CurrentTime 0 2]];\r\
  \n:local Min [:tostr [:pick \$CurrentTime 3 5]];\r\
  \n:local Day [:tostr [:pick \$CurrentDate 4 6]];\r\
  \n:local Month [:tostr [:pick \$CurrentDate 0 3]];\r\
  \n:local Year [:tostr [:pick \$CurrentDate 7 [:len \$CurrentDate]]];\r\
  \n:global name=backupfile value=([/system identity get name] .\"__\$Day_\$\
  Month_\$Year__\$Hour_\$Min.backup\")\r\
  \n:global name=scriptfile value=([/system identity get name] .\"__\$Day_\$\
  Month_\$Year__\$Hour_\$Min.rsc\")\r\
  \n/system backup save name=\$backupfile;\r\
  \n/export verbose file=\$scriptfile;\r\
  \n:delay 10s\r\
  \n/tool fetch address=<SERVER> src-path=\$backupfile user=<USER>\
  r mode=ftp password=<PASSWORD> dst-path=\"backup/\$backupfil\
  e\" upload=yes;\r\
  \n/tool fetch address=<SERVER> src-path=\$scriptfile user=<USER>\
  r mode=ftp password=<PASSWORD> dst-path=\"backup/\$scriptfil\
  e\" upload=yes;\r\
  \n:delay 20s\r\
  \n/file remove \$backupfile;\r\
  \n/file remove \$scriptfile;\r\
  \n/log info \"backup finished\";\r\
  \n"
```