Инструкция по конфигурированию Mikrotik RouterOS для работы в сети интернет-провайдера Корбина Телеком (Билайн)

Контактные данные:

Сайт — *http://minirouter.ru*
e-mail — *support@minirouter.ru*

Инструкция проверена на моделях роутеров Mikrotik RB750, RB750G, RB450, RB450G с прошивками версий 4.6, 4.10, 4.11 и 5.22.

История изменений документа:

- Версия 0.8 от 01.03.2013 — рекомендованный remote-address изменён с адреса из локальной подсети 127.0.2.1 на адрес из приватной подсети 192.168.255.254 . Протестировано на RouterOS 5.22 (это устраняет несовместимость с новыми версиями RouterOS). В образцах команд консоли убраны приглашения, для облегчения копирования и вставки в терминал. Исправлен копирайт.
- Версия 0.7 от 07.07.2011 — рекомендованный remote-address изменён с адреса из приватной подсети 192.168.200.1 на адрес из локальной подсети 127.0.2.1. Протестировано на RouterOS 5.4.
- Версия 0.6 от 20.10.2010 — Исправлена ошибка с метрикой маршрутов по умолчанию в DHCP Client, приводившая к отсутствию связи после изменения конфигурации корбины (ориентировочно 18.10.2010).
- Версия 0.5 от 15.08.2010 — Исправлены задания в планировщике. Добавлена инструкция по включению NAT на интерфейсе corbina-l2tp. Добавлены указания по добавлению маршрутов к DNS серверам.
- Версия 0.4 от 14.08.2010 — Удалены пробелы в конце строк в многострочных скриптах.
- Версия 0.3 от 12.08.2010 — Исправлена ошибка использования несоответствия используемого имени профиля при создании профиля и l2tp подключения.
- Версия 0.2 от 24.06.2010 — Исправлены опечатки в примерах команд.
- Версия 0.1 от 23.06.2010 — Начальная редакция документа.

Введение

Настройки роутеров Mikrotik для работы с интернет-провайдером Корбина Телеком (Билайн) имеет ряд особенностей, обусловленных архитектурой сети провайдера.

В частности:

1. У Корбины Телеком не настроены маршруты к vpn серверам. Поэтому, после установления vpn соединения и последующей активации шлюза по умолчанию, для установленного vpn соединения пропадает связь с vpn сервером и тоннель внутри vpn-соединения рвётся.
2. В качестве RemoteIP внутри тоннеля Корбина-Телеком выдаёт ip-адрес vpn-сервера к которому происходит подключение. В сочетании со статическими маршрутами к vpn-серверам это также нарушает маршрутизацию через тоннель.
3. Корбина Телеком осуществляет балансировку нагрузки на vpn-сервера с помощью ротации серверов через DNS (так называемый round robin dns). Первичная настройка vpn-соединения происходит нормально, но роутер Mikrotik в конфигурации vpn-соединения (в текущей версии Mikrotik RouterOS) запоминает ip адрес конкретного vpn-сервера. Это приводит к потере связи при остановке данного vpn-сервера, поскольку автоматическое переключение на альтернативные сервера не происходит.

Первая проблема решается добавлением статических маршрутов к vpn серверам.
Вторая проблема решается подменой RemoteIP в тоннеле на приватный адрес из неиспользуемой подсети (например 192.168.255.254).
Третья проблема решается созданием скрипта, регулярно проверяющего состояние vpn-соединения, и производящего повторное преобразование имени vpn сервера в ip-адрес и переконфигурирование vpn-соединения в случае прерывания связи.

Пример настройки роутера

Рассмотрим настройку роутера для работы в сети Корбина Телеком на конкретном примере.

Перед подключением к сети провайдера, убедитесь что пароли пользователей в роутере Mikrotik заменены на безопасные и/или файрвол блокирут подключения к роутеру из публичной сети. Настройка по умолчанию в RB/750, RB/750G, RB/MRT и RB/MRTG блокирует все входящие подключения с интерфейса *ether1-gateway*, но не блокирует остальные интерфейсы включая создаваемые vpn-подключения.

Предполагаем что настройки IP для внутренней сети сделаны и безопасность обеспечена.

Подключаем кабель сети Корбина Телеком в порт *eth1* роутера.

Убедимся что DHCP-client для интерфейса *ether1-gateway* работает и получил настройки ip для локальной сети Корбина Телеком.

```
[admin@MikroTik] > /ip dhcp-client print detail
Flags: X - disabled, I - invalid
 0   ;;; default configuration
     interface=ether1-gateway host-name="rssonhome" add-default-route=yes
     default-route-distance=1 status=bound address=10.73.250.237/21
     dhcp-server=83.102.233.200 primary-dns=85.21.192.3
     secondary-dns=213.234.192.8 expires-after=6d23h40m23s
```

Установим для полученного по DHCP маршрута по умолчанию, метрку больше чем будет у маршрута по умолчанию у vpn подключения.

```
/ip dhcp-client set ether1-gateway default-route-distance=2
```

Включим DNS в роутере. В качестве серверов указываем *primary-dns* и *secondary-dns* из полученных параметров dhcp (эта настройка может не требоваться, поскольку можт быть выполнене автоматически dhcp клиентом при включённой опции Peer DNS).

```
[admin@] > /ip dns set servers=85.21.192.3,213.234.192.8 allow-remote-requests=yes
```

После этого DNS должен работать. Проверяем:

```
:ping www.ru
194.87.0.50 ping timeout
194.87.0.50 ping timeout
194.87.0.50 ping timeout
3 packets transmitted, 0 packets received, 100% packet loss
```

Видно что преобразование имени *www.ru* в адрес *194.87.0.50* произошло. но ping на внешний ip невозможен, поскольку vpn еще не настроен.

В некотрых сегментах сети Корбина может не работать из за отсутствия маршрута к DNS серверам. Маршруты к DNS серверам добавляются аналогично маршрутам к VPN серверам.

Для того чтобы добавить маршруты к vpn серверам, определим их адреса. В ОС Microsoft Windows это осуществляется командой:

Для pptp тоннеля:

```
C:\>nslookup vpn.internet.beeline.ru
       :  router
Address:  192.168.1.4
```

Получаем такой ответ (от не заслуживающего доверия dns-сервера):

```
         :  vpn.internet.beeline.ru
Addresses:  85.21.0.105
            85.21.0.117
            78.107.1.48
            85.21.0.226
```

Аналогично для l2tp тоннеля:

```
C:\>nslookup tp.internet.beeline.ru
       :  router
Address:  192.168.1.4
Ответ (от не заслуживающего доверия dns-сервера):
         :  tp.internet.beeline.ru
Addresses:  85.21.0.241
            85.21.0.243
```

В данном случае все сервера находятся в двух подсетях
85.21.0.0/24
78.107.1.0/24

Для добавления маршрутов на эти подсети требуется выяснить ip-адрес-шлюза в локальной сети Корбина Телеком. Его можно найти в любом из маршрутов добавленных автоматически при DHCP настройке.

```
[admin@MikroTik] > /ip route print detail
...
 6 ADS  dst-address=10.0.0.0/8 gateway=10.73.248.1
        gateway-status=10.73.248.1 reachable ether1-gateway distance=1 scope=30
        target-scope=10 ...
```

Искомый маршрут отмечен флагами *ADS* и адрес шлюза лежит в локальной подсети Корбина Телеком.

Добавляем маршруты на эту подсеть через шлюз в локальной сети Корбина Телеком:

```
[admin@MikroTik] > /ip route
[admin@MikroTik] > add comment="vpn servers subnet" dst-address=78.107.1.0/24 \
    gateway=10.73.248.1
[admin@MikroTik] > add comment="vpn servers subnet" dst-address=85.21.0.0/24 \
    gateway=10.73.248.1
```

Теперь создадим профиль соединения для Корбина Телеком. В нем укажем *remote-address* произвольно из неиспользуемых приватных подсетей:

```
/ppp profile
 add change-tcp-mss=yes comment="" name=Corbina only-one=default \
 remote-address=192.168.255.254 use-compression=no use-encryption=no use-vj-
compression=no
```

Создадим l2tp-подключение. В параметры *user* и *password* вместо *corbinauser* и *password* надо указать ваш логин и пароль в Корбине для установления подключения, а в качестве connect-to один из ip-адресов в которые разрешалось имя tp.internet.beeline.ru :

```
[admin@MikroTik] > /interface l2tp-client add name=corbina-l2tp profile=Corbina \
    user=corbinauser password=password \
    connect-to=85.21.0.241 disabled=no add-default-route=yes\
    max-mru=1420 max-mtu=1420 mrru=disabled
```

И добавляем правило NAT для интерфейса VPN

```
[admin@MikroTik] > /ip firewall nat add out-interface=corbina-l2tp \
    chain=srcnat action=masquerade
```

Теперь роутер подключен к Интернет .

Чтобы автоматизировать действия по восстановлению vpn- соединения в случае обрыва/дисконнекта, добавим скрипты для обновления ip- адреса vpn-сервера:

```
/system script
add name=corbina-l2tp_soft_refresh policy=ftp,read,write,winbox source=":local\
    \_interface \"corbina-l2tp\"\r\
    \n:local vpnserver \"tp.internet.beeline.ru\"\r\
    \n#:log debug message=\"Soft resolv script run\"\r\
    \n:if ([/interface l2tp-client get \$interface running] = false) do={\r\
    \n   :log info message=\"VPN down. Refreshing\"\r\
    \n   /ip dns cache flush\r\
    \n   :local \"current-ip\" [:resolve \$vpnserver]\r\
    \n   :local \"old-ip\" [/interface l2tp-client get [/interface l2tp-client\
    \_find name=\"\$interface\"] connect-to]\r\
    \n   :if (\$\"current-ip\" != \$\"old-ip\") do= {\r\
    \n      :log info \"VPN Server changed IP address from \$\"old-ip\" to \$\
    \"current-ip\"\"\r\
    \n      /interface l2tp-client set [/interface l2tp-client find name=\"\$i\
    nterface\"] connect-to=\$\"current-ip\"\r\
    \n   }\r\
    \n}"
add name=corbina-l2tp_refresh policy=ftp,read,write,winbox source=":local inte\
    rface \"corbina-l2tp\"\r\
    \n:local vpnserver \"tp.internet.beeline.ru\"\r\
    \n:log debug message=\"Hard resolv script run\"\r\
    \n#:if ([/interface l2tp-client get \$interface running] = false) do={\r\
    \n   /ip dns cache flush\r\
    \n   :local \"current-ip\" [:resolve \$vpnserver]\r\
    \n   :local \"old-ip\" [/interface l2tp-client get [/interface l2tp-client\
    \_find name=\"\$interface\"] connect-to]\r\
    \n   :if (\$\"current-ip\" != \$\"old-ip\") do= {\r\
    \n      :log info \"VPN Server changed IP address from \$\"old-ip\" to \$\
    \"current-ip\"\"\r\
    \n      /interface l2tp-client set [/interface l2tp-client find name=\"\$i\
    nterface\"] connect-to=\$\"current-ip\"\r\
    \n   }\r\
    \n#}"
```

И финальный штрих - добавляем задания в планировщик заданий роутера:

```
/system scheduler
add disabled=no interval=1s name=corbina-l2tp_soft_refresh \
    on-event="/system script run corbina-l2tp_soft_refresh" \
    policy=reboot,read,write,policy,test \
    start-time=00:00:00
add disabled=no interval=0s name=corbina-l2tp_refresh \
    on-event="/system script run corbina-l2tp_refresh" \
    policy=reboot,read,write,policy,test \
    start-time=04:30:00
```

В результате, скрипт *corbina-l2tp_soft_refres*h выполняется каждую секунду, и обновляет ip только если vpn-соединение неактивно, а скрипт *corbina-l2tp_refresh* выполняется каждый день в 4:30, при этом соединение пере-устанавливается.

Замечания, вопросы и предложения по данной инструкции пожалуйста отправляйте по электронной почте на адрес *support@minirouter.ru*.