Мне понадобилось использовать роутер mikrotik в качестве клиента openvpn с заменой шлюза по-умолчанию на сервер openvpn. Проще говоря мне нужно было скрыть весь трафик и направить его только через vpn сервер. В openvpn это реализуется очень просто, достаточно на сервере указать для конкретного пользователя параметр redirect-gateway def1. На клиенте под windows это без проблем работает. В микротике пришлось разбираться.

> Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую пройти курсы по программе, основанной на информации из официального курса MikroTik Certified Network Associate. Все подробности читайте ниже.

Содержание:

Введение

Расскажу для чего мне это нужно. Есть оператор Yota с безлимитным интернетом за разумные деньги. У них есть разные тарифы в зависимости от устройства, в котором используется симка. Самый дешевый тариф для смартфона. Я купил обычный USB модем, разлочил его, чтобы он работал в сети Yota. Перепрошил специальной прошивкой, чтобы он стал похож на смартфон. Пишу очень просто, потому что не хочется на этом останавливаться. Это совсем другая тема. В интернете есть много информации на тему обхода блокировок yota. Подробнее об этом я рассказал отдельно в материале Настройка интернета в загородном доме — mikrotik + usb 4g lte модем + антенна MIMO для усиления сигнала + yota.

Мне нужно было замаскировать весь трафик локальной сети, которая будет пользоваться интеренетом через usb модем. Yota различными способами пытается бороться с подобной работой. Делается это через определние TTL пакетов и анализ ресурсов, к которым обращаются пользователи. TTL легко изменяется на конечных устройствах, либо на самом роутере. С анализом ресурсов я долгое время боролся редактируя файл hosts, но после установки windows 10 это перестало помогать. Винда постоянно куда-то лезла и идентифицировала себя при этом как компьютер, а не смартфон.

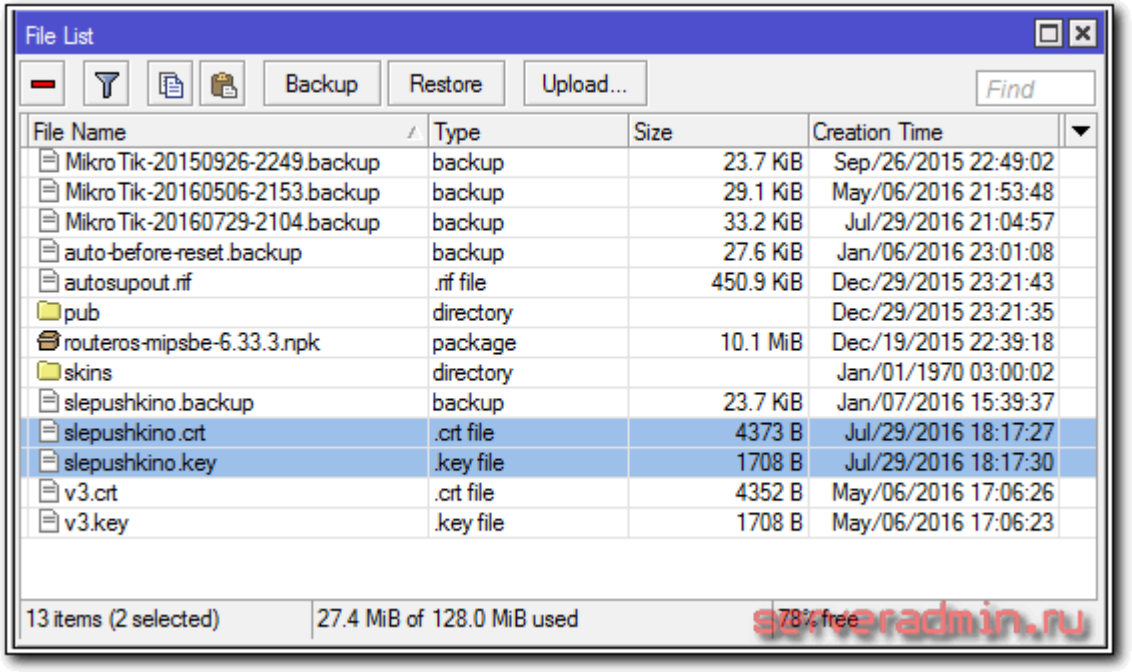
Я решил кардинально решить проблему и завернуть весь локальный трафик в шифрованный vpn туннель. Для этого настроил openvpn сервер и сделал конфигурацию для учетной записи с заменой шлюза по-умолчанию на openvpn сервер. Дальше нужно было настроить на miktotik openvpn клиент таким образом, чтобы он весь трафик заворачивал в vpn. Когда используешь windows клиент, ничего настраивать не надо. Указываешь на openvpn сервере настройку у клиента:

```
push "redirect-gateway def1 bypass-dhcp"
```

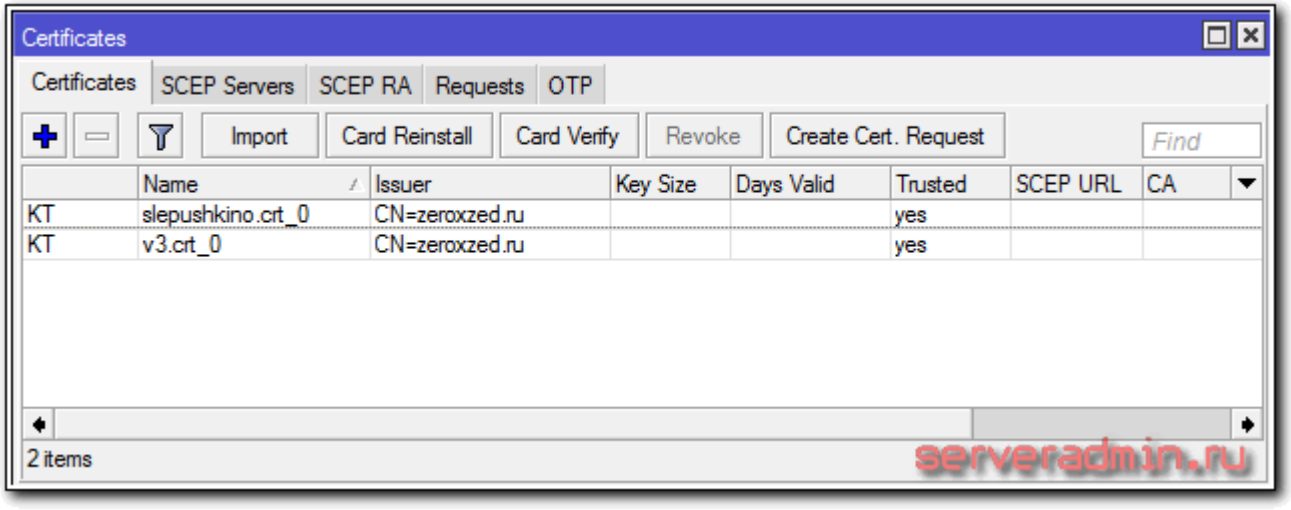
И все, при подключении все маршруты прописываются как надо и твой внешний ip при серфинге становится равен ip адресу openvpn сервера. Весь трафик идет в тоннель. На микротике это не работало, маршруты надо было писать вручную. Получилось у меня не сразу, расскажу обо всем по порядку.

Настройка openvpn клиента на mikrotik

Настраиваем стандартным образом подключение openvpn клиента к серверу с авторизацией по сертификату. Для этого берем сертификат и приватный ключ для openvpn клиента и копируем на микротик через стандартное средство просмотра файлов **Files**:

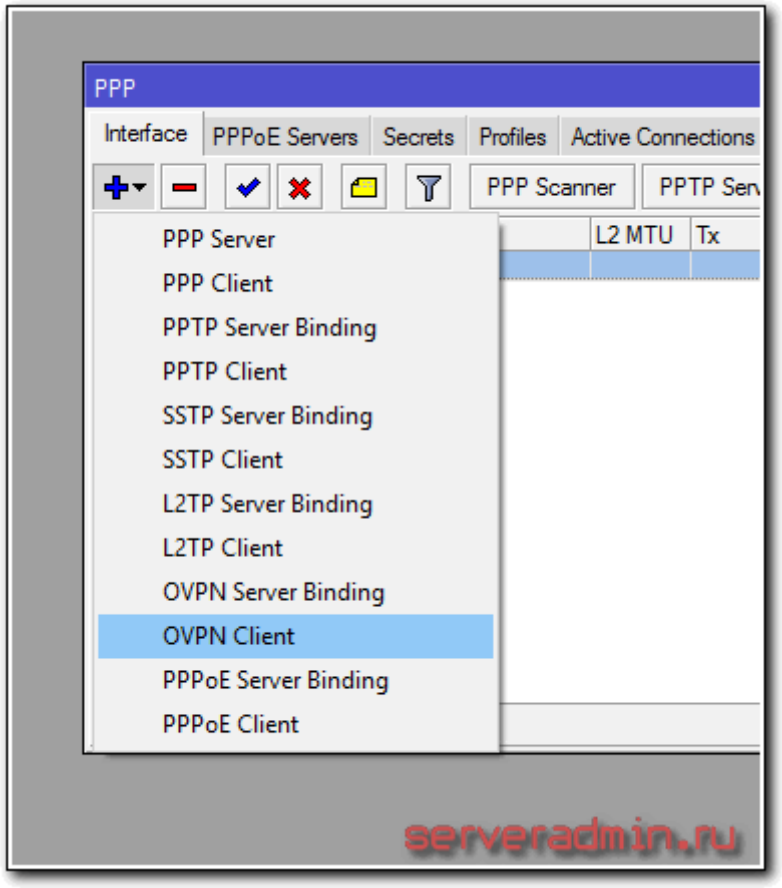


Потом идем в **System -> Certificates** и имортируем по очереди сначала сертификат, а потом приватный ключ:

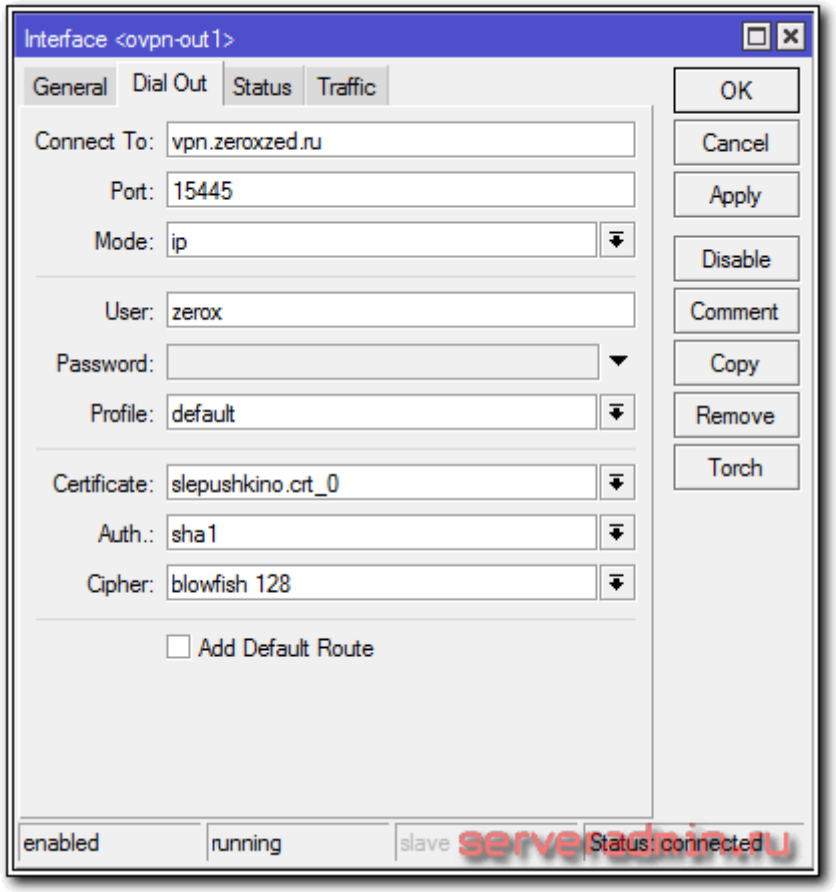


Обращаю внимание на символы KT слева от названий сертификатов. Они обязательно должны быть у вас. Если сертификат и приватный ключ не соответствуют друг другу, то одного символа не будет. В моем примере уже есть 2 сертификата только потому, что я экспериментировал с двумя. Вам достаточно будет одного.

Дальше идем настраивать параметры сервера. Открываем разздел **PPP**, нажимаем на плюс и выбираем **OVPN Client**:



На вкладке General можно ничего не указывать, использовать все по-умолчанию. На следующей вкладке Dial Out указываем адрес vpn сервера, порт, на котором он принимает входящие соединения и сертификат. Все остальное можно не трогать. В поле User можно писать все, что угодно.



Сохраняете подключение. Теперь клиент на микротике должен автоматически подключиться к openvpn серверу. Если этого не происходит, смотрите в чем проблема в логах на роутере или на сервере. На данном этапе все стандартно, должно заработать без проблем. Инструкций по этому вопросу в интернете море.

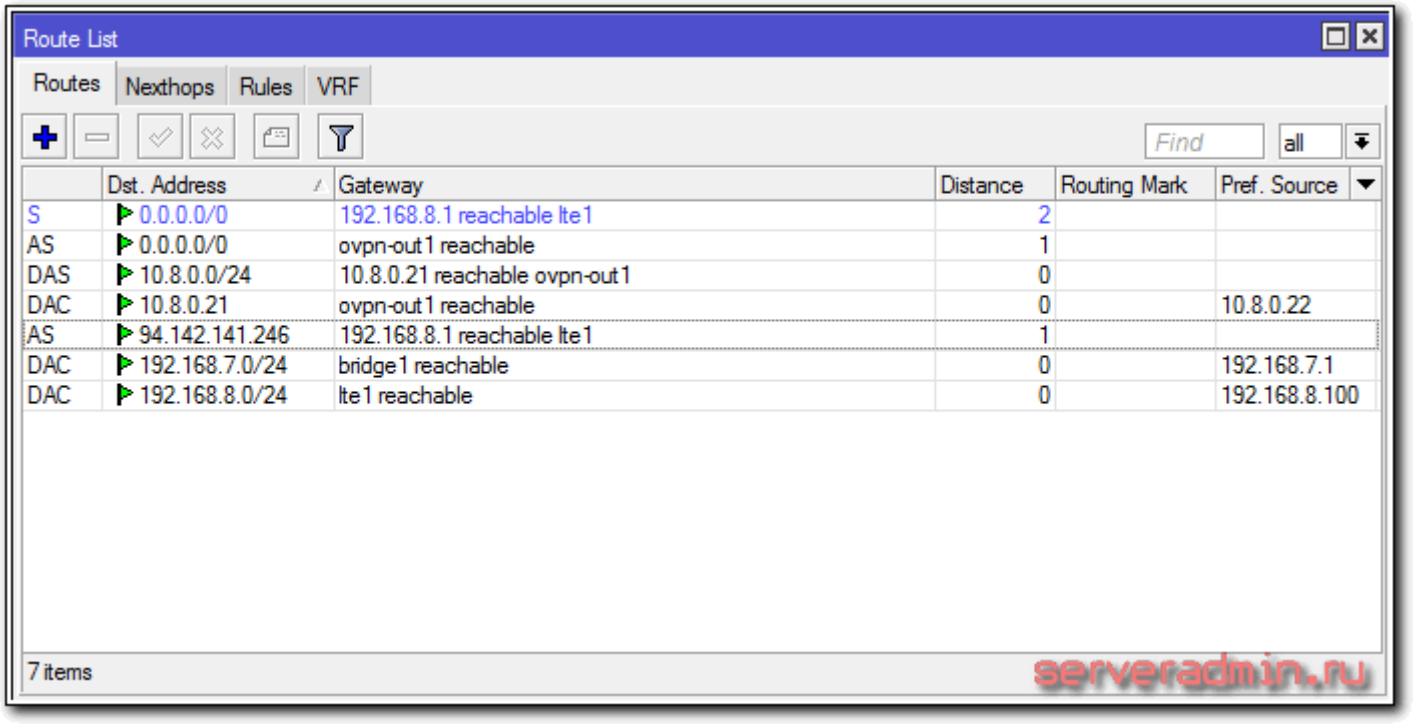
Замена шлюза по-умолчанию для маскировки всего трафика

Настройка на сервере для клиента, которая указывает заменять шлюз по-умолчанию, на микротике не работает. Если указать в настройках openvpn сервера галочку на параметре **Add Default Route**, то тоже ничего работать не будет. Просто не будет пускать в интернет. Хотя для меня это было не понятно. По идее, это как раз то, что нужно. Не могу сейччас привести скриншот маршрутов, коотрые будут прописаны, если установить эту галку. Я пишу статью, подключившись к роутеру удаленно, скрин сделать не могу, потеряю доступ.

Я могу привести только гарантированно работающий вариант. Сейчас расскажу смысл проделанного и приведу список маршрутов, которые добавил.

1. Первым делом создаем маршрут до openvpn сервера с Distance 1.
2. Маршуруту по-умолчанию, который обеспечивает доступ в интернет через usb модем, назначаем Distance 2.
3. Создаем новый маршрут по-умолчанию с Distance 1, где в качестве шлюза указано openvpn подключение.

После этого вы будете иметь доступ в интернет через usb модем напрямую, если openvpn client будет отключен. После подключения vpn клиента к серверу, стандартный маршрут становится неактивным, а по-умолчанию становится новый маршрут со шлюзом в качестве vpn соединения. Весь ваш трафик будет замаскирован vpn соединением и пойдет через openvpn сервер.



Описание маршрутов

0.0.0.0/0	192.168.8.1	Стандартный маршрут по-умолчанию, когда не подключен openvpn
0.0.0.0/0	ovpn-out1	Маршрут по-умолчанию через vpn сервер
10.8.0.0/24	10.8.0.21	Автоматически создаваемый маршрут для подссети vpn тоннелей
10.8.0.21	ovpn-out1	То же самое, автоматически создаваемый маршрут
94.142.141.246	192.168.8.1	Маршрут к openvpn server через usb модем
192.168.7.0/24	bridge1	Маршурт для локальной сети, создается автоматически
192.168.8.0/24	lte1	Маршрут до usb модема, создается автоматически

- 192.168.8.1 — адрес usb модема, 192.168.8.100 — адрес микротика на lte интерфейсе, к которому подключен модем
- 192.168.7.1 — адрес микротика в локальной сети
- 10.8.0.21 — адрес vpn тоннеля для данного клиента, адрес самого клиента при этом 10.8.0.22
- 94.142.141.246 — openvpn server

> Когда будете настраивать, не забудте включить NAT на openvpn интерфейсе, так же как у вас он настроен на основном.

Заключение

С такими настройками мне удалось обеспечить интернетом весь загородный дом с помощью симки йоты для смартфона, usb модема, внешней антенны для усиления сигнала и роутера mikrotik. Ссылку на подробный рассказ о моей конфигурации я привел в начале статьи. Без антенны вообще без вариантов было, еле-еле ловил 3g. С антенной стал ловить 4g со скоростью до 5-ти мегабит, если вышка не забита. В час пик скорость все равно не очень, но хоть что-то. Дом далеко от вышек сотовых сетей, без антенны интернет не работает ни у одного оператора.

Онлайн курсы по Mikrotik

Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую пройти курсы по программе, основанной на информации из официального курса MikroTik Certified Network Associate. Помимо официальной программы, в курсах будут лабораторные работы, в которых вы на практике сможете проверить и закрепить полученные знания. Все подробности на сайте Курсы по ИТ. Стоимость обучения весьма демократична, хорошая возможность получить новые знания в актуальной на сегодняшний день предметной области.