Настройка OpenVPN Сервера и Клиента на MikroTik

mikrotiklab.ru/nastrojka/artga-openvpn.html

January 20, 2020

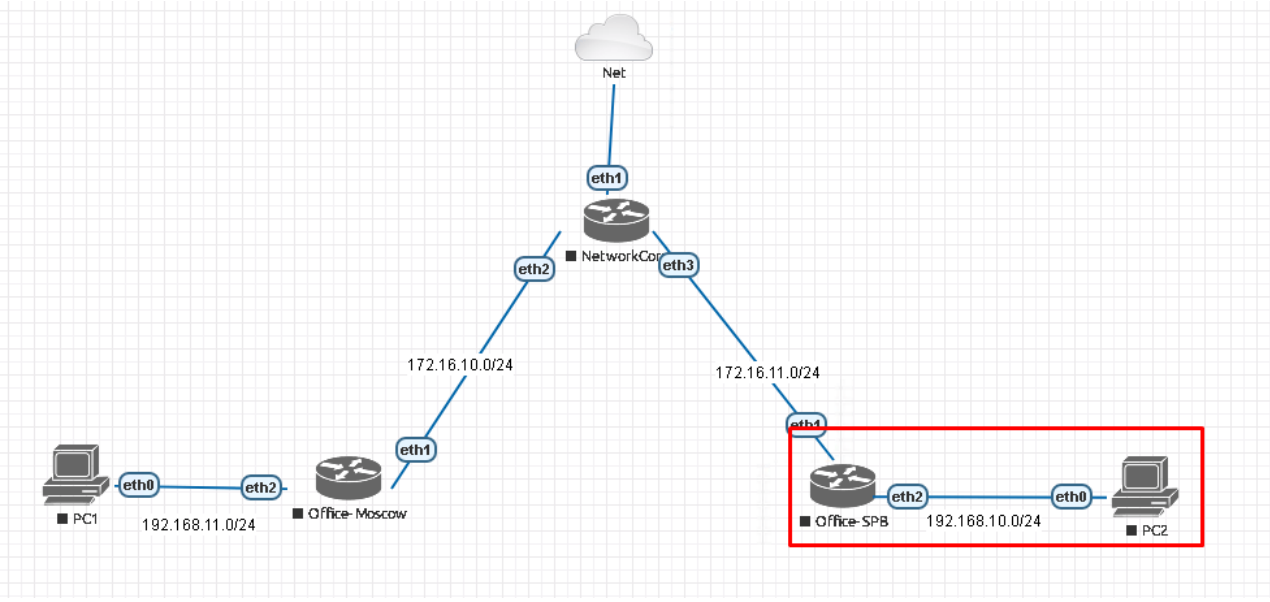
В данной инструкции я покажу настройку между двумя Mikrotik OpenVPN Server и Client. Будем делать аутентификацию без сертификата и с ним. Конфигурация с сертификатами требует большой подготовки и ответственности, так как нам нужно всегда думать о сохранности, актуальности и списке отзыва, но не оспоримый плюс — это высокая безопасность. Правилом хорошего тона будет постоянный экспорт сертификатов из роутера на внешнее хранилище, жесткий диск.

Стоит иметь что на оборудовании Mikrotik отсутствуют какие-либо чипы аппаратной разгрузки для OpenVPN. В связи с этим вся нагрузка будет идти через центральный процессор, а значит, что скорость соединений напрямую зависит от загруженности роутера.

Так же OpenVPN на RouterOS v6 не поддерживает следующее:

- UDP протокол, т.е. необходимо использовать исключительно TCP;
- LZO сжатие;
- TLS аутентификация;
- Аутентификация без имени пользователя и пароля;

Схема сети представлена ниже.



Приняв во внимание вышеописанные ограничения и особенности приступим к настройке.
Мы находимся справа внизу в офисе SPB (Office-SPB).
Вводные данные:

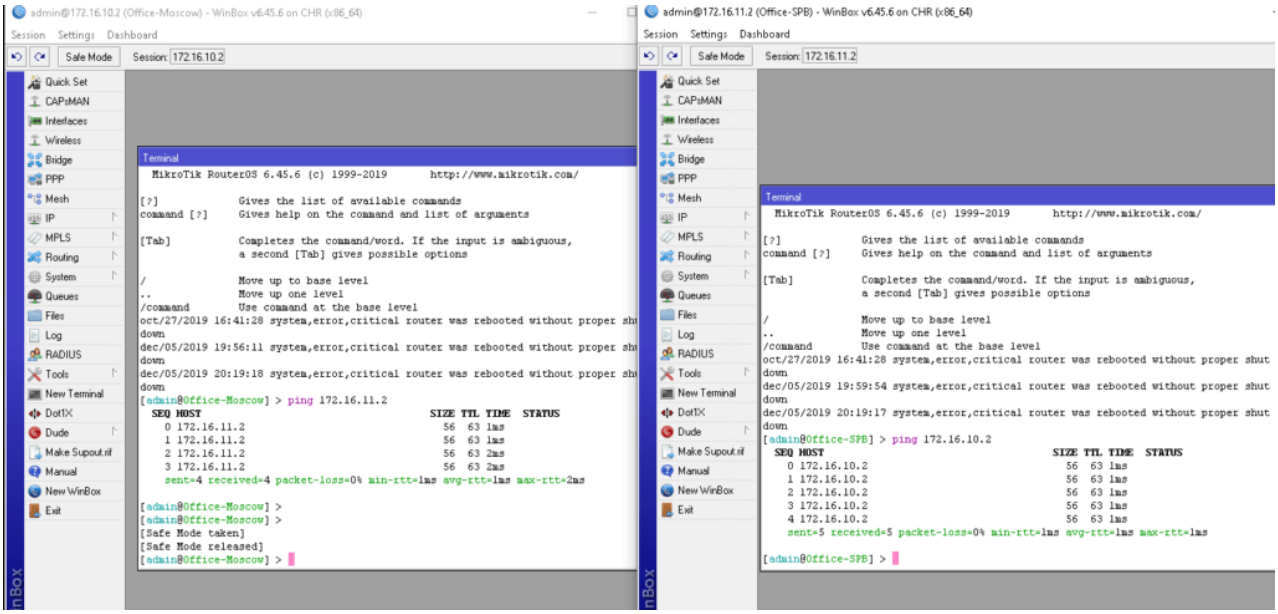
- Office-SPB сервер;
- Office-Moscow клиент;
- NetworkCore выполняет роль провайдера, он будет заниматься обычной маршрутизацией;
- Office-Moscow ether1 смотрит в интернет 172.16.10.2/24;
- Office-SPB ether1 смотрит в интернет 172.16.11.2/24;
- Office-Moscow имеет bridge “General-Bridge” в локальной сети 192.168.11.1/24;
- Office-SPB имеет bridge “General-Bridge” в локальной сети 192.168.10.1/24;
- IP ПК в локальной сети Office-Moscow 192.168.11.2;
- IP ПК в локальной сети Office-SPB 192.168.10.2;
- Адресация в VPN сети 172.16.25.0/24;
- Версии RouterOS 6.46.2.

Наша команда рекомендует изучитьНаша команда рекомендует изучить углубленный курс по администрированию сетевых устройств MikroTik В курсе много лабораторных работ по итогам которых вы получите обратную связь. После обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно тут.

Содержание

Настройка OpenVPN по логину и паролю

Первым делом проверим доступность через интернет. Я отправлю ping запросы с обоих роутеров, чтобы убедиться, что они друг друга видят. В реальной жизни один из них должен иметь белый (публичный) IP, а именно тот, кто будет выполнять роль сервера.

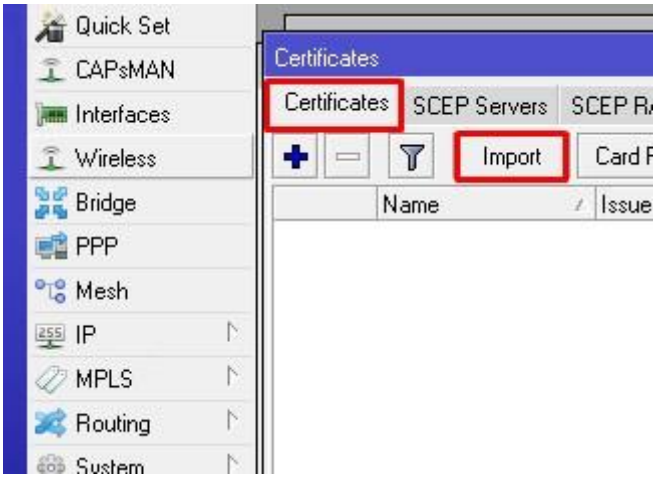


Создание сертификата центра сертификации

На московском роутере открываем System — Certificates.

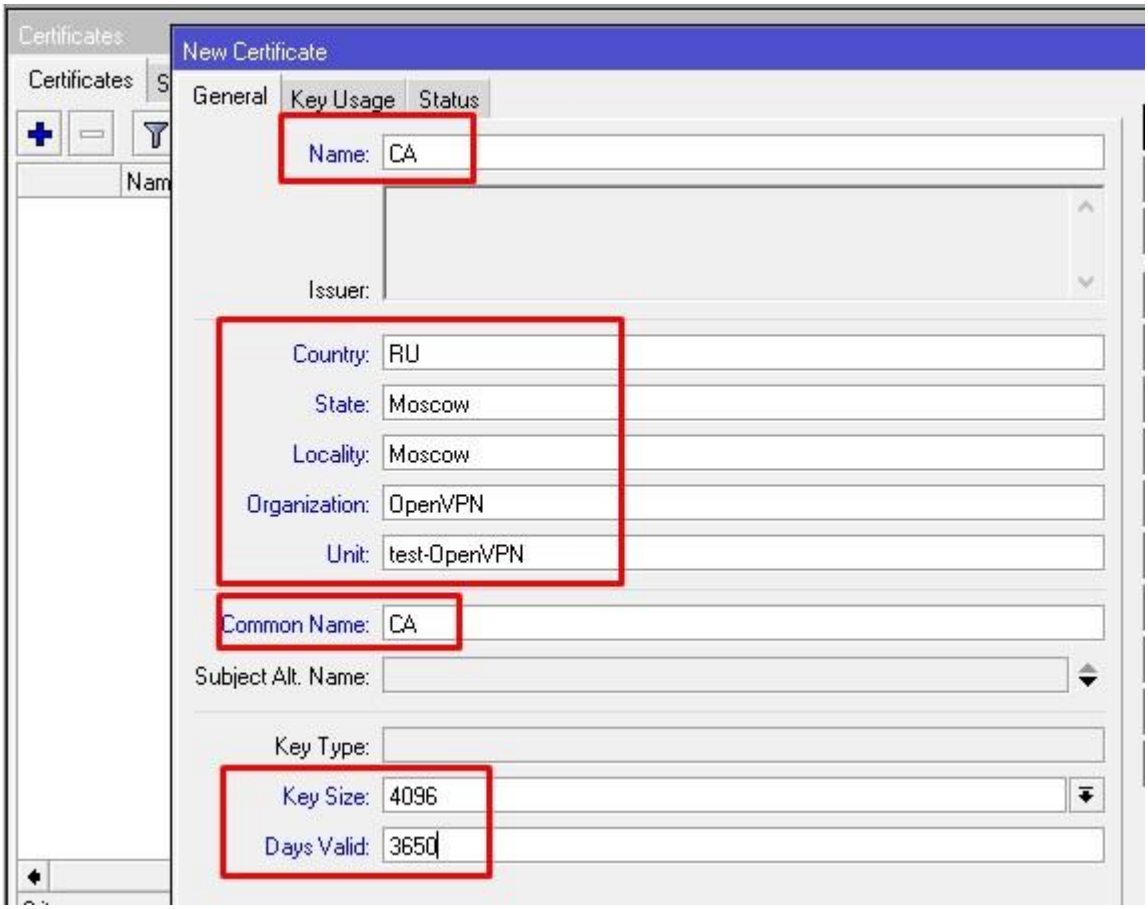
В данном разделе находятся все сертификаты на Mikrotik. Для настройки сервера нам необходимо сделать следующее:

- Создать сертификат центра сертификации;
- Создать сертификат сервера.



Нажимаем плюс и задаем параметры согласно скриншоту:

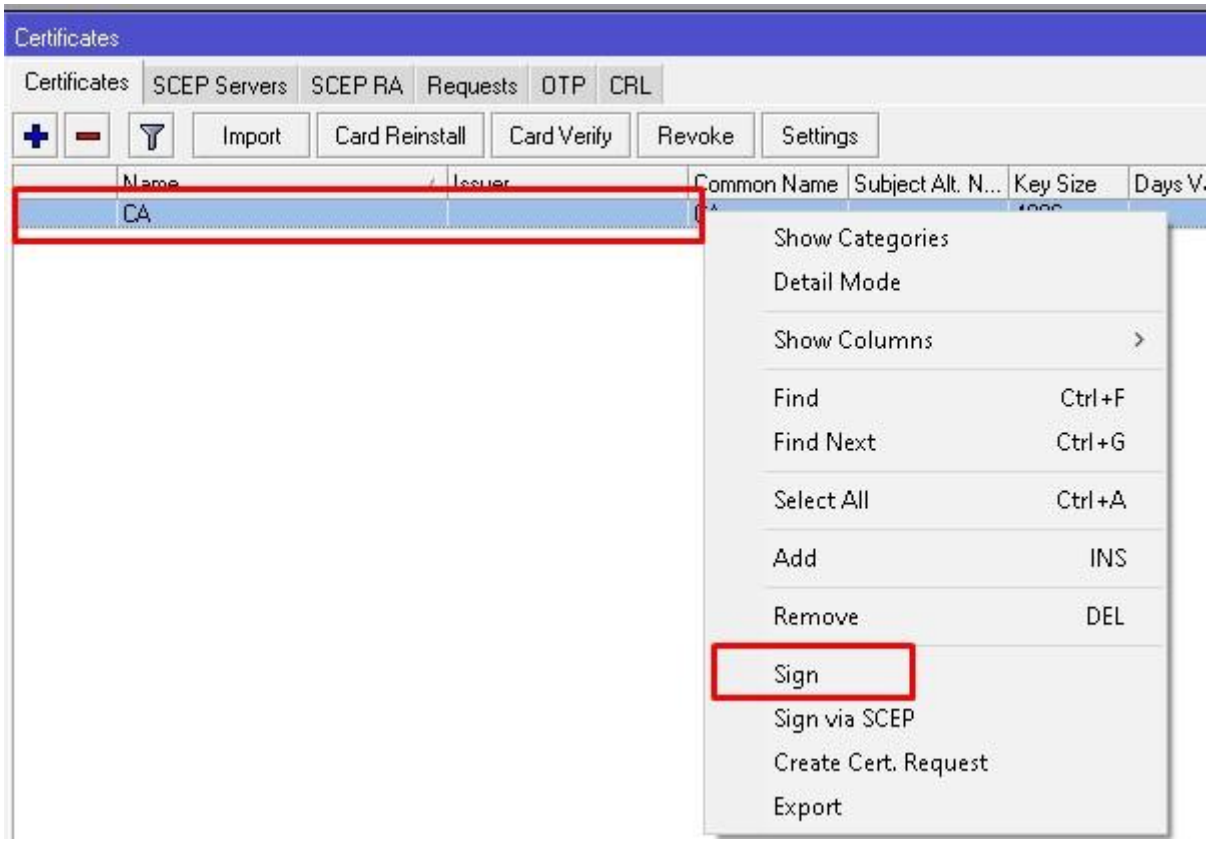
- Name – имя в списке Mikrotik;
- Country, Sate, Locality, Organization, Unit – произвольные поля для заполнения;
- Common Name – самое важное. Указываем уникальное имя;
- Key Size – длина ключа. Выбирается в выпадающем списке;
- Days Valid – срок годности.



На данный момент мы создали шаблон.

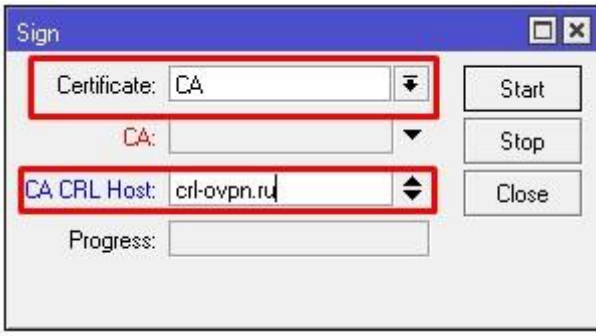
> Подписание**!** Обращаю внимание, что мы будем создавать самоподписанный корневой сертификат центра сертификации.

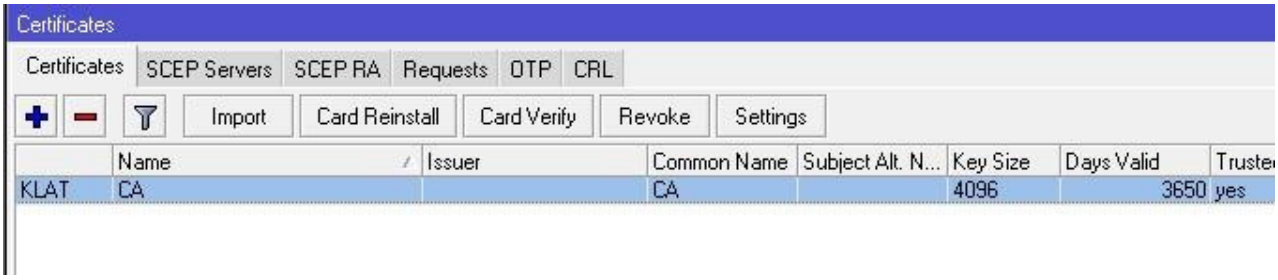
Ничего страшного в этом нет, т.к. мы не собираемся его использовать для других сервисов. Выбираем наш шаблон, и в контекстном меню выбираем Sign.



В открывшемся окне выбираем CA. Обязательно указываем CA CRL Host – список отзыва, можно указать доменное имя.

Нажимаем Start и ждем окончания процесса.

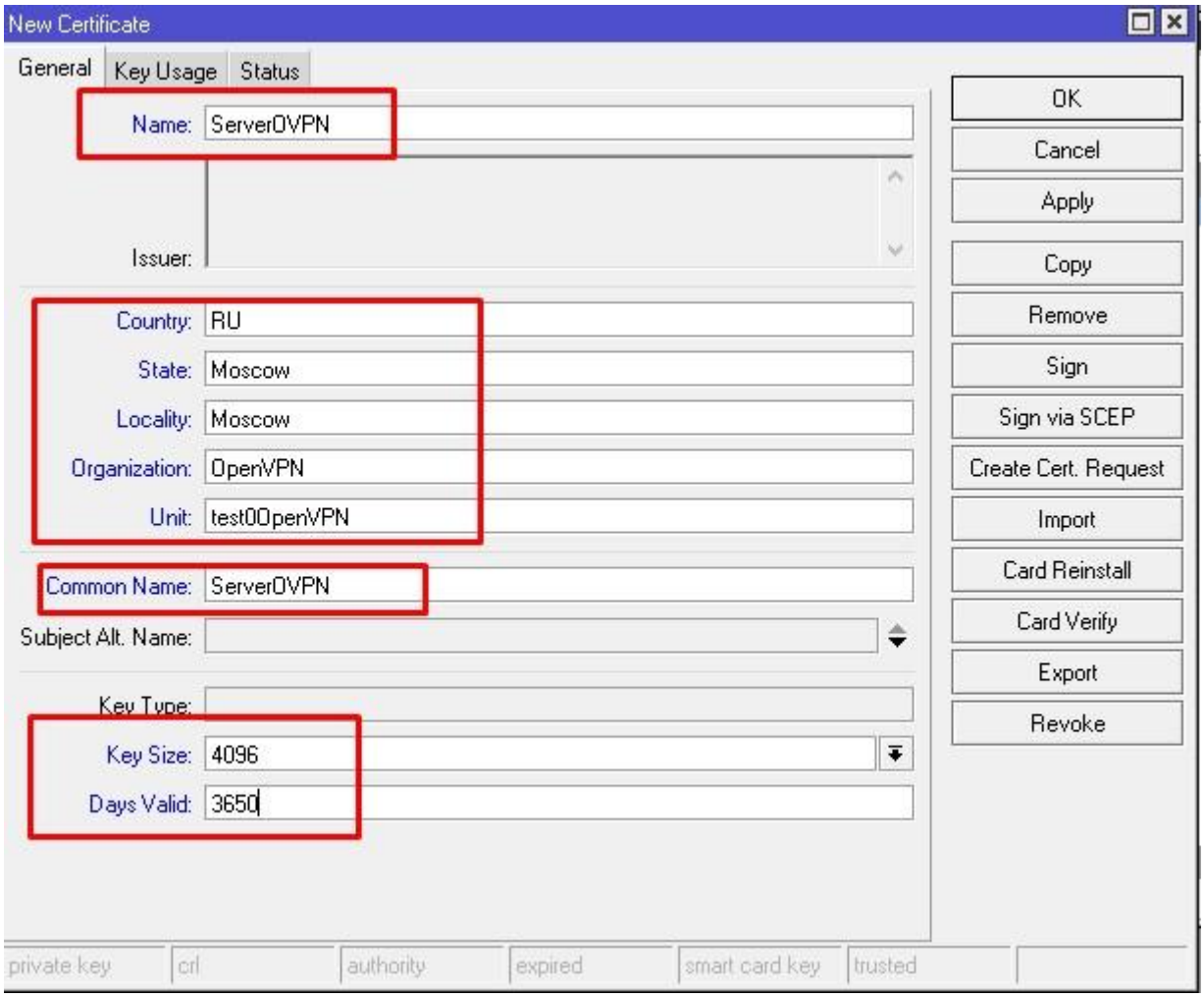




Создание сертификата сервера OpenVPN

Открываем Certificates и нажимаем на плюс.

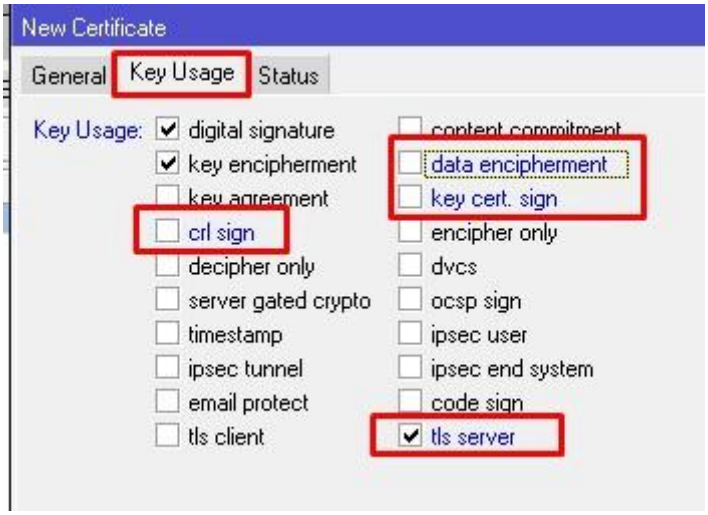
Указываем уникальные имя и Common Name.



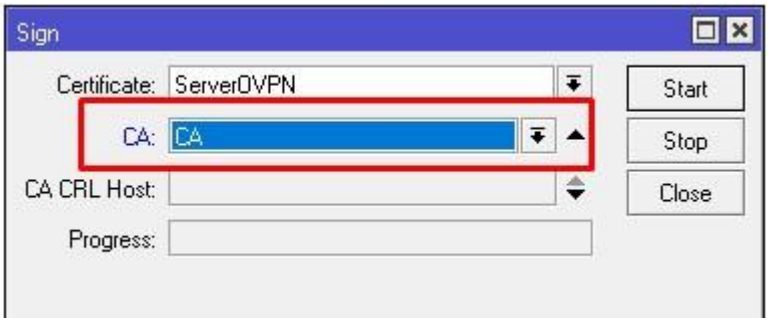
Открываем Key Usage, снимаем галочки с:

- crl sign;
- data encipherment;
- key sert sign;
- ставим галочку на tls server.

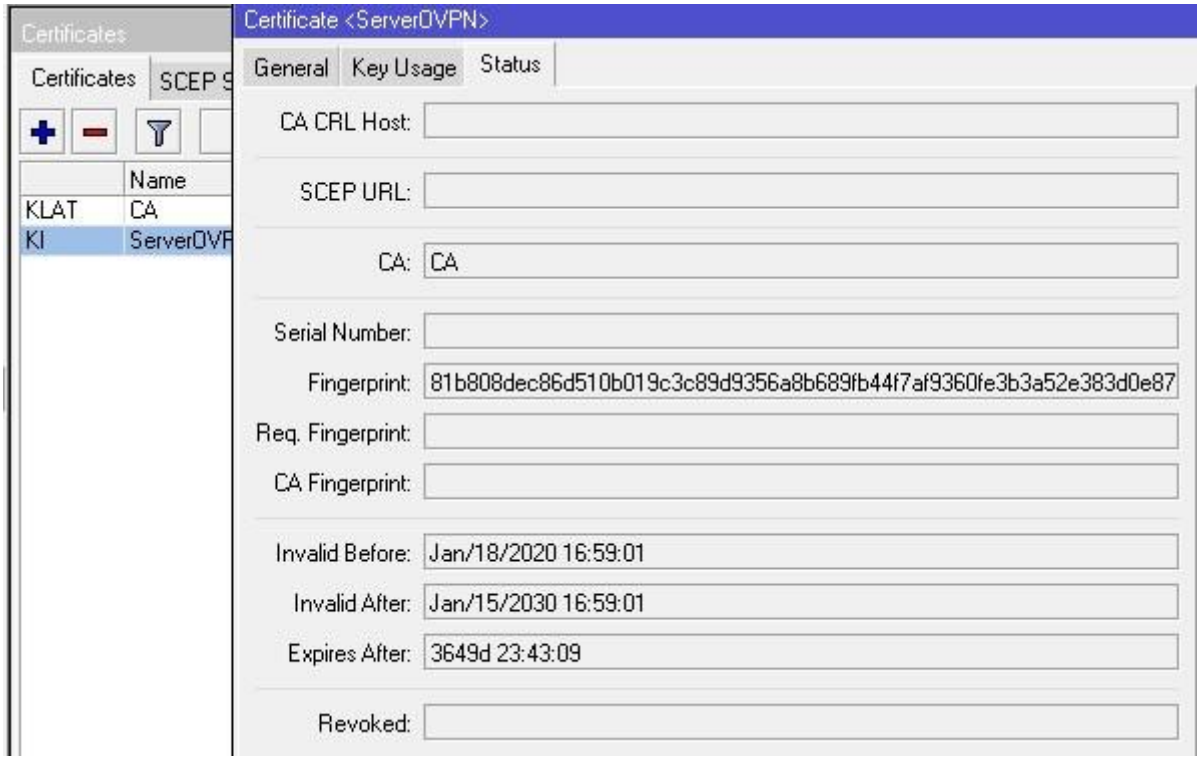
Сохраняем. Переходим к подписанию.



Выбираем сертификат в списке. В контекстном меню нам нужен Sign. В Certificate выбираем шаблон ServerOVPN, в CA самоподписанный корневой сертификат. Start.

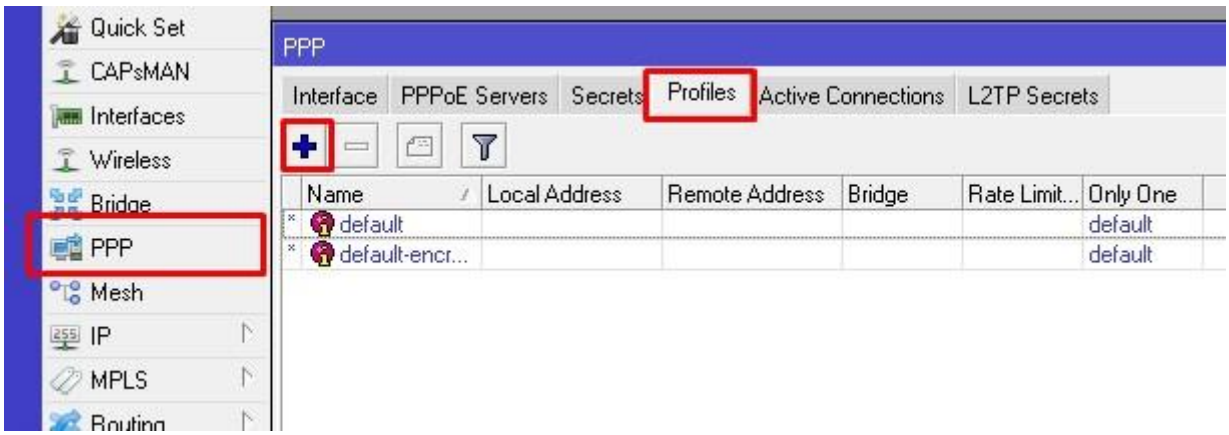


В списке видим, что наш шаблон превратился в полноценный сертификат. Можем открыть его свойства.



Конфигурирование сервера

Но для начала создадим профиль. PPP – Profiles – жмем +.



Перед нами открывается окно нового профайла. В строке «Name» задаем понятное нам имя. В строке Local Address указываем IP адрес Mikrotik в VPN. Я указываю 172.16.25.1. Т.е. при подключении клиента автоматически присвоится именно это

адрес.

Далее переключаем:

- Change TCP MSS в yes.
- Use UPnP переключаем в no.

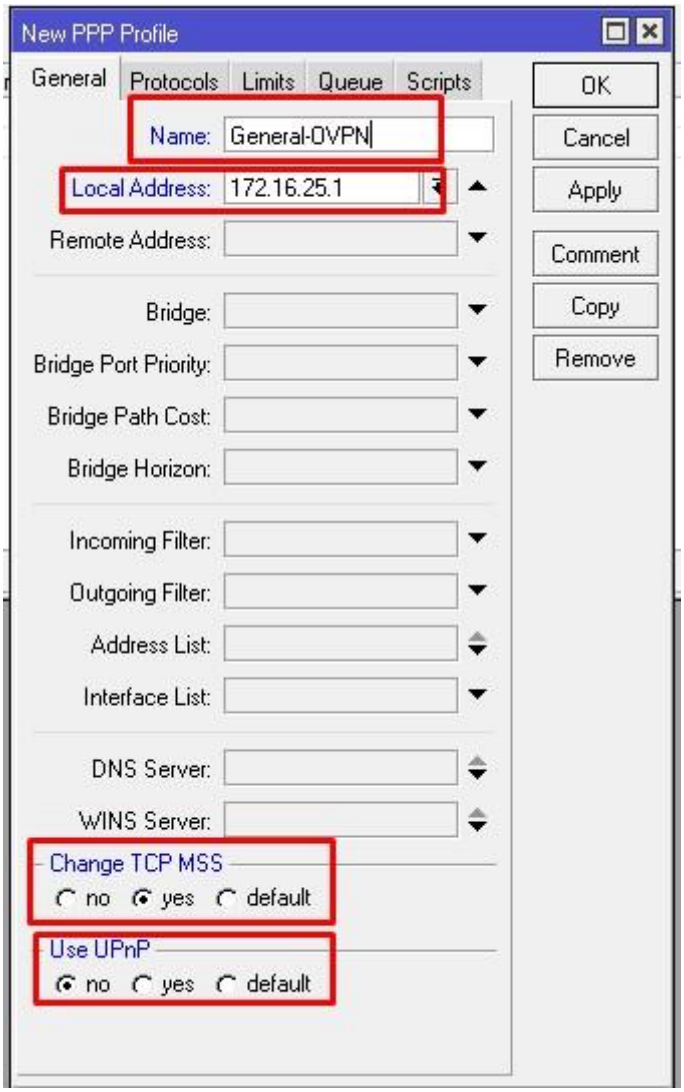
> Никогда не оставляйте default если хотите, чтобы все работало именно так, как вы планируете.

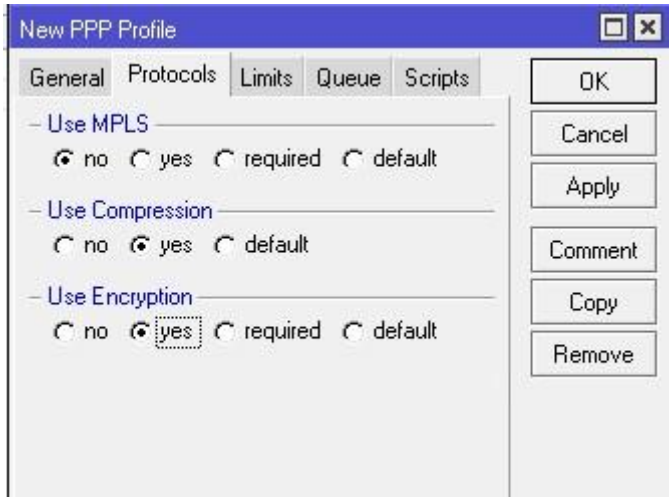
Protocols:

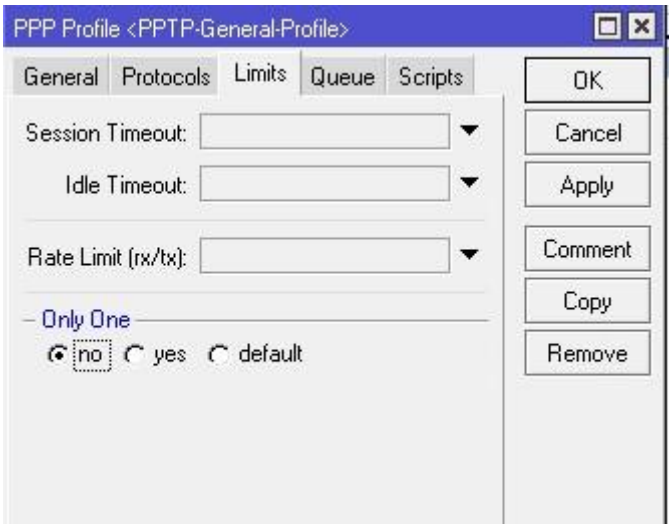
- no для Use MPLS;
- yes для Use Compression;
- yes для Use Encryption.

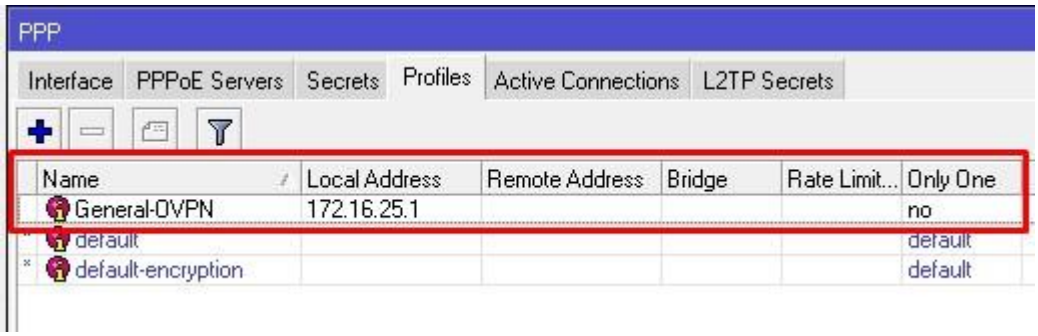
Далее в Limits ставим no для Only One. Остальные настройки можно не задавать. К примеру, если бы нам нужно было ограничить скорость клиента внутри тоннеля, то нас интересовала вкладка Queue – но это совсем другая история.

Теперь можно сохранять. Жмем Apply и OK. В списке должен появиться наш созданный профиль.

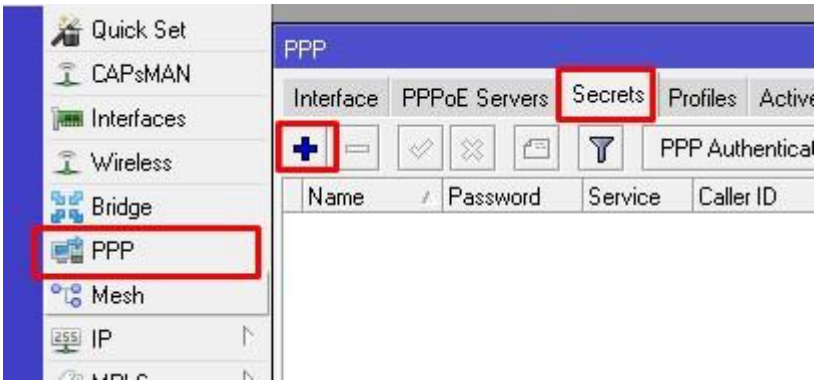






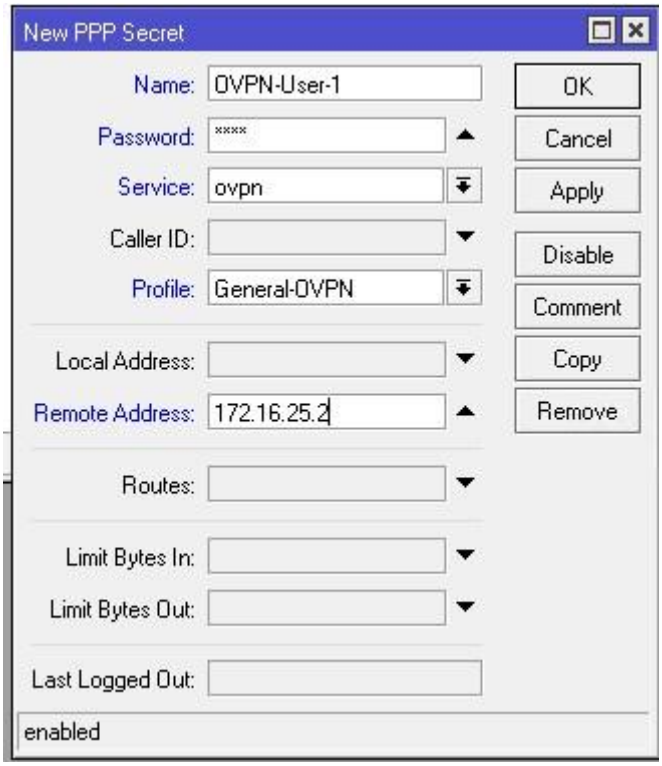


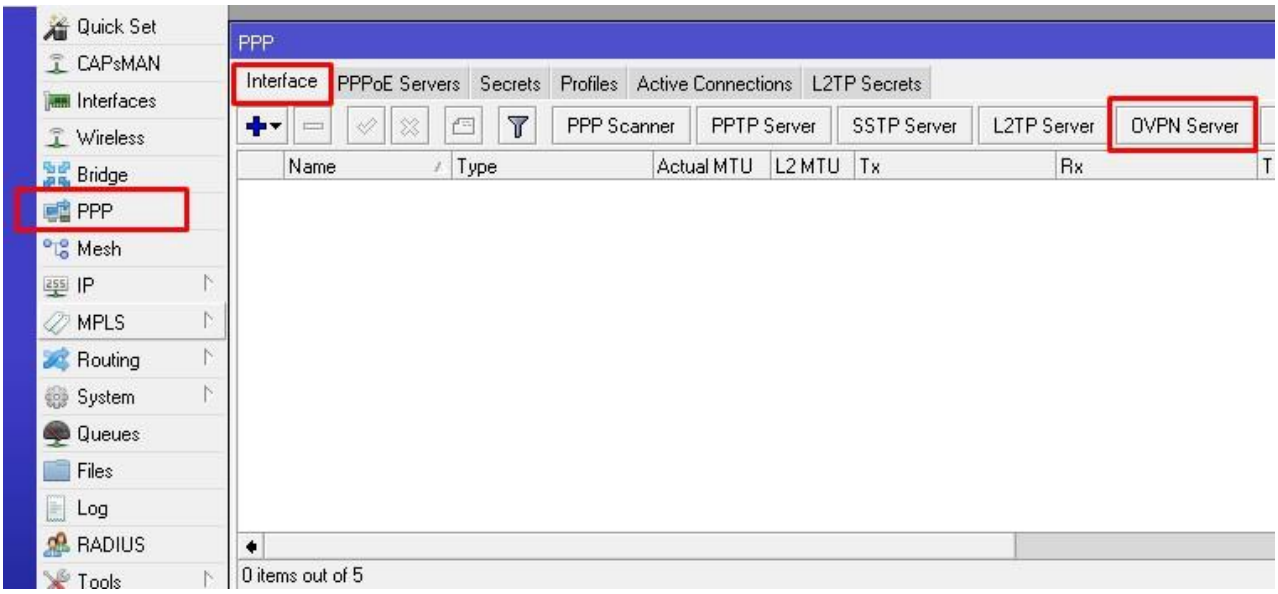
Нам нужно создать пользователя и пароль, который будет подключаться к нашей сети. Открываем Secrets и жмем +.



Задаем произвольные логин и пароль. Выбираем Service – ovpn, Profile – General-OVPN, Remote Address – 172.16.25.2 т.к. я планирую подключать одного пользователя (рекомендую использовать привязку по IP если хотите гибко управлять Firewall в отношении каждого пользователя). Если вам нужно больше одного, то необходимо создать DHCP Pool. Apply и Ok.

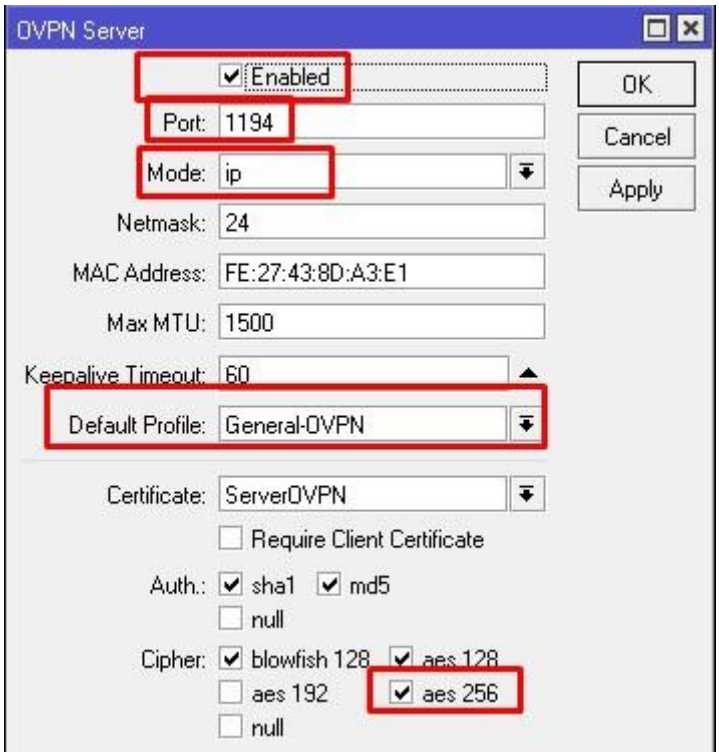
Открываем PPP – Interfaces – OPENV Server.





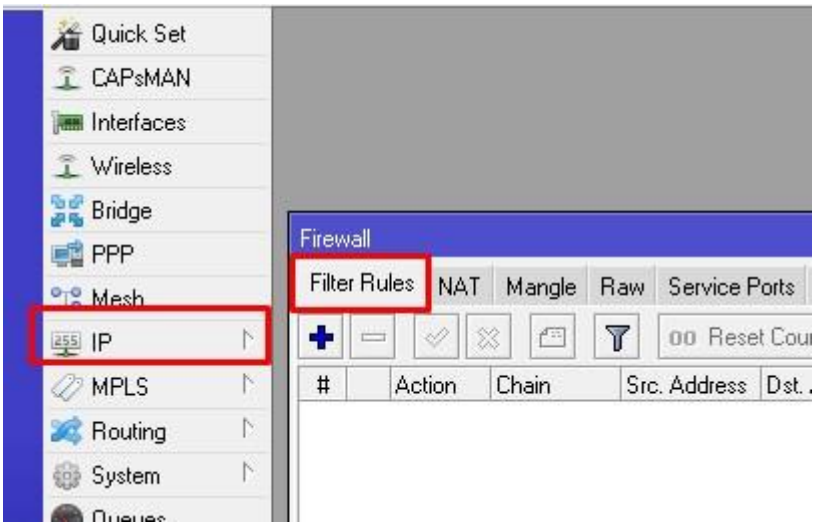
- Ставим галочку Enable;
- Задаем порт (не забываем, что это TCP);
- Mode – ip;
- Default Profile – созданный ранее профайл General-OVPN;
- Certificate – сертификат сервера ServerOVPN;
- Cipher – aes256.

Apply и Ok.

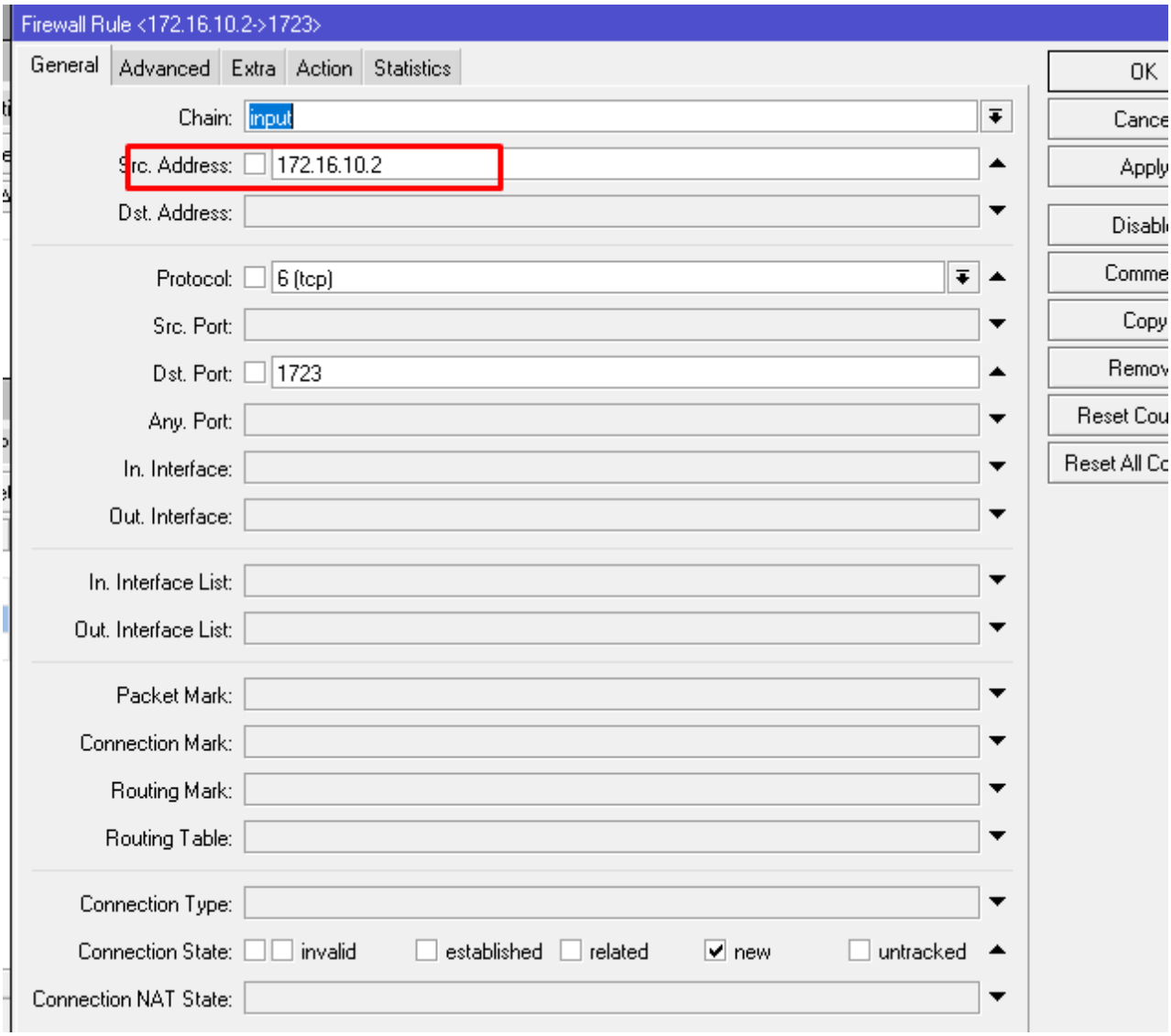


Настройка Firewall

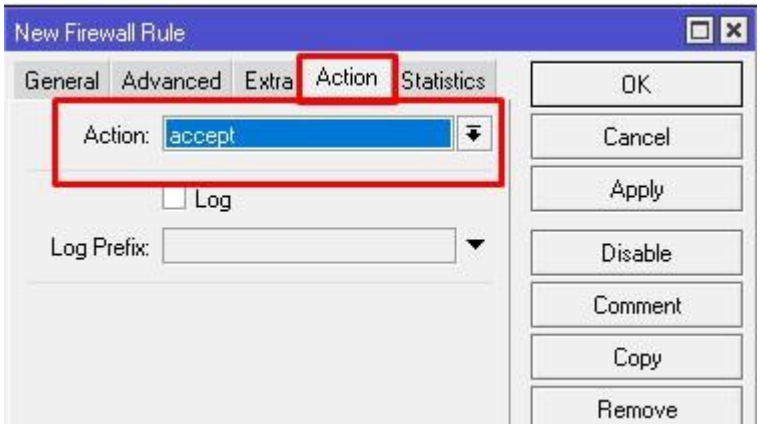
Далее нужно разрешить OpenVPN трафик на роутере.



Добавляем правило.



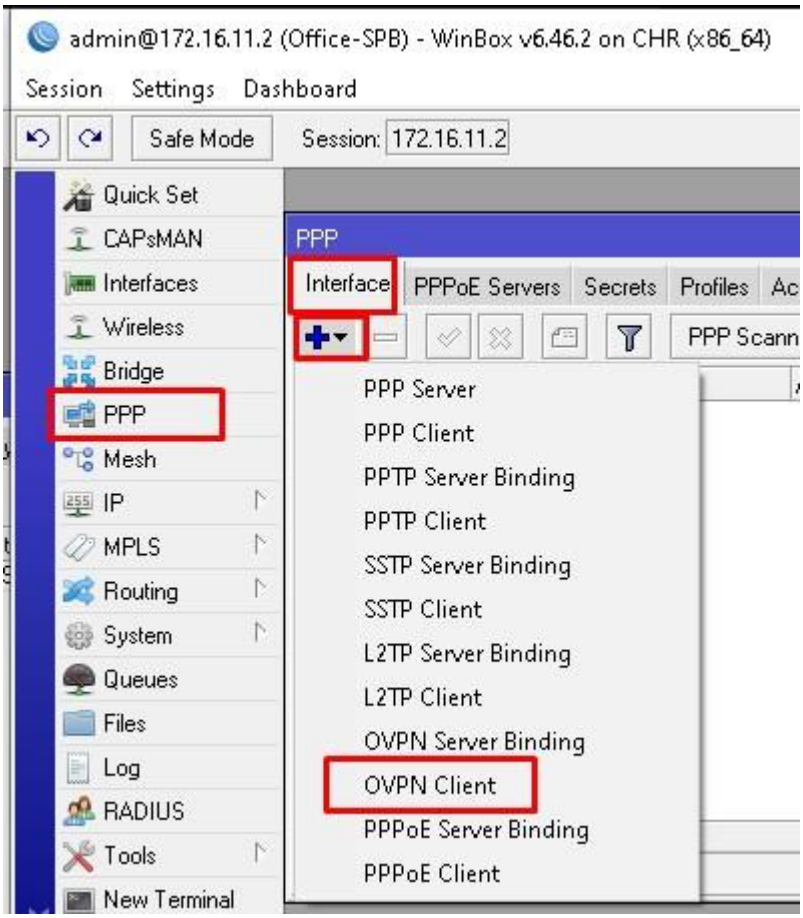
Action – accept.



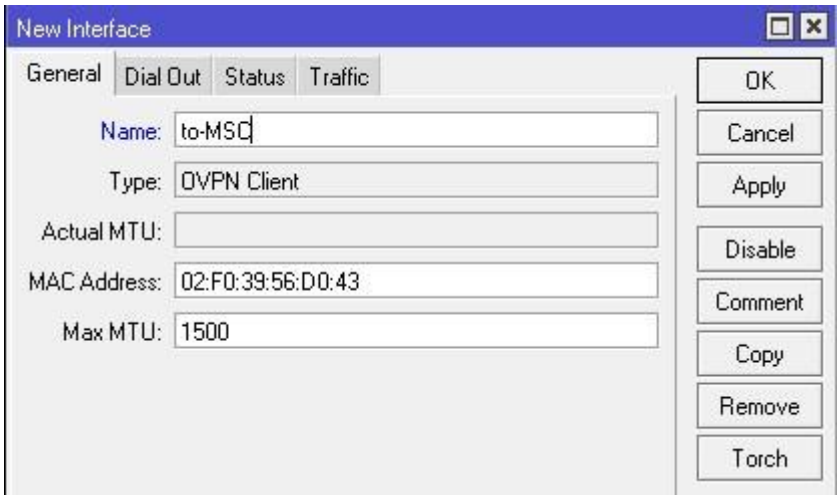
Сохраняем и переходим к клиентской части.

Конфигурирование клиента

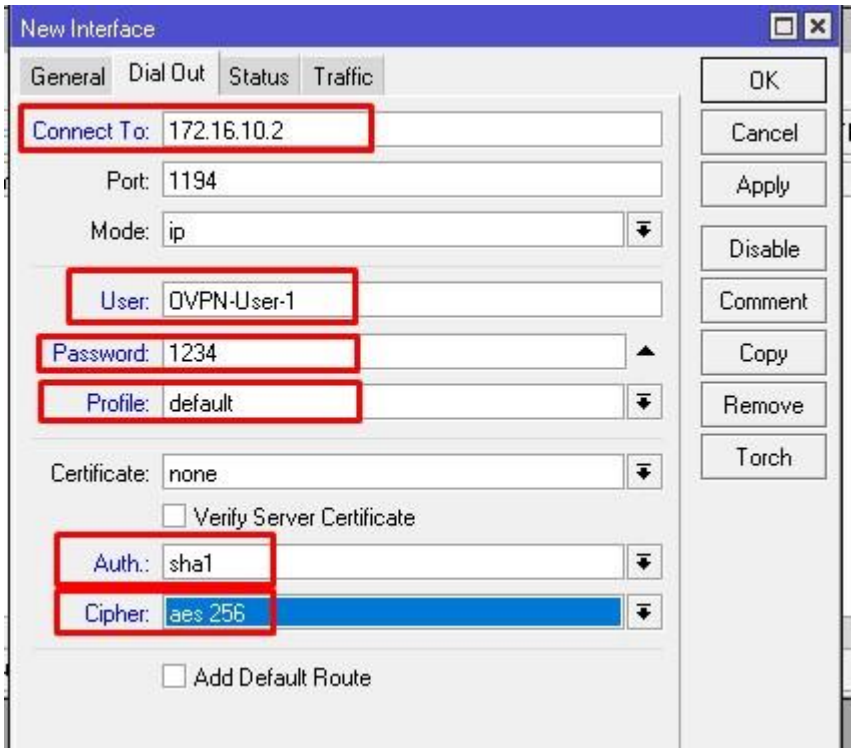
Подключаемся к питерскому роутеру и в PPP создаем новый интерфейс OVPN Client.



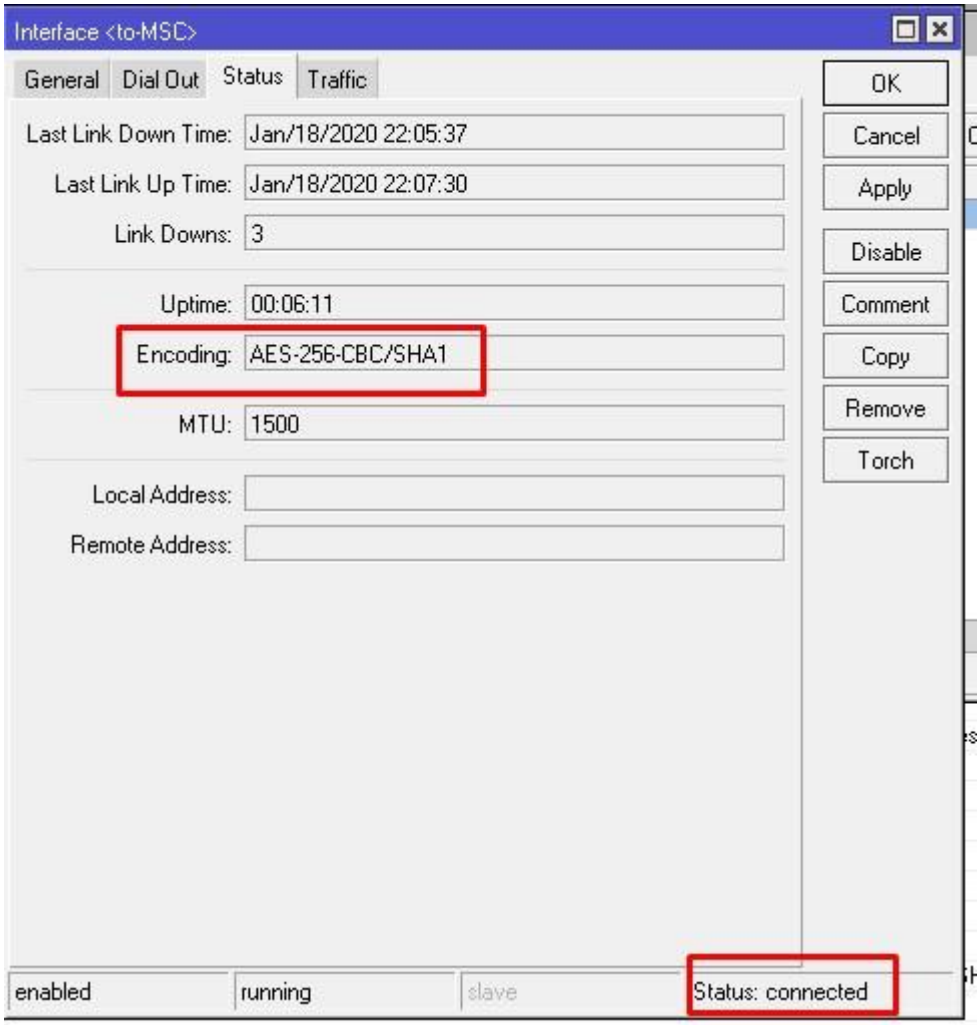
Задаем имя интерфейса.



Открываем Dial Out и заполняем обязательные параметры.



Сохраняем и открываем вкладку Status.



Здесь мы видим статус подключено, шифрование и время жизни соединения. Вы спросите, а где же IP адрес клиента? Он по каким-то причинам не отображается в окне статуса интерфейса, зато есть в IP-Address. Возможно, ошибка, в данной прошивке. Попробуем проверить доступность московского роутера через VPN.

```
/command        Use command at the base level
[admin@Office-SPB] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    172.16.11.2/24     172.16.11.0     ether1
 1    192.168.10.1/24    192.168.10.0    General-Bridge
 2 D  172.16.25.2/24     172.16.25.0     to-MSC
[admin@Office-SPB] > ping 172.16.25.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 172.16.25.1                                56  64 1ms
    1 172.16.25.1                                56  64 3ms
    2 172.16.25.1                                56  64 1ms
    3 172.16.25.1                                56  64 27ms
    sent=4 received=4 packet-loss=0% min-rtt=1ms avg-rtt=8ms max-rtt=

[admin@Office-SPB] >
```

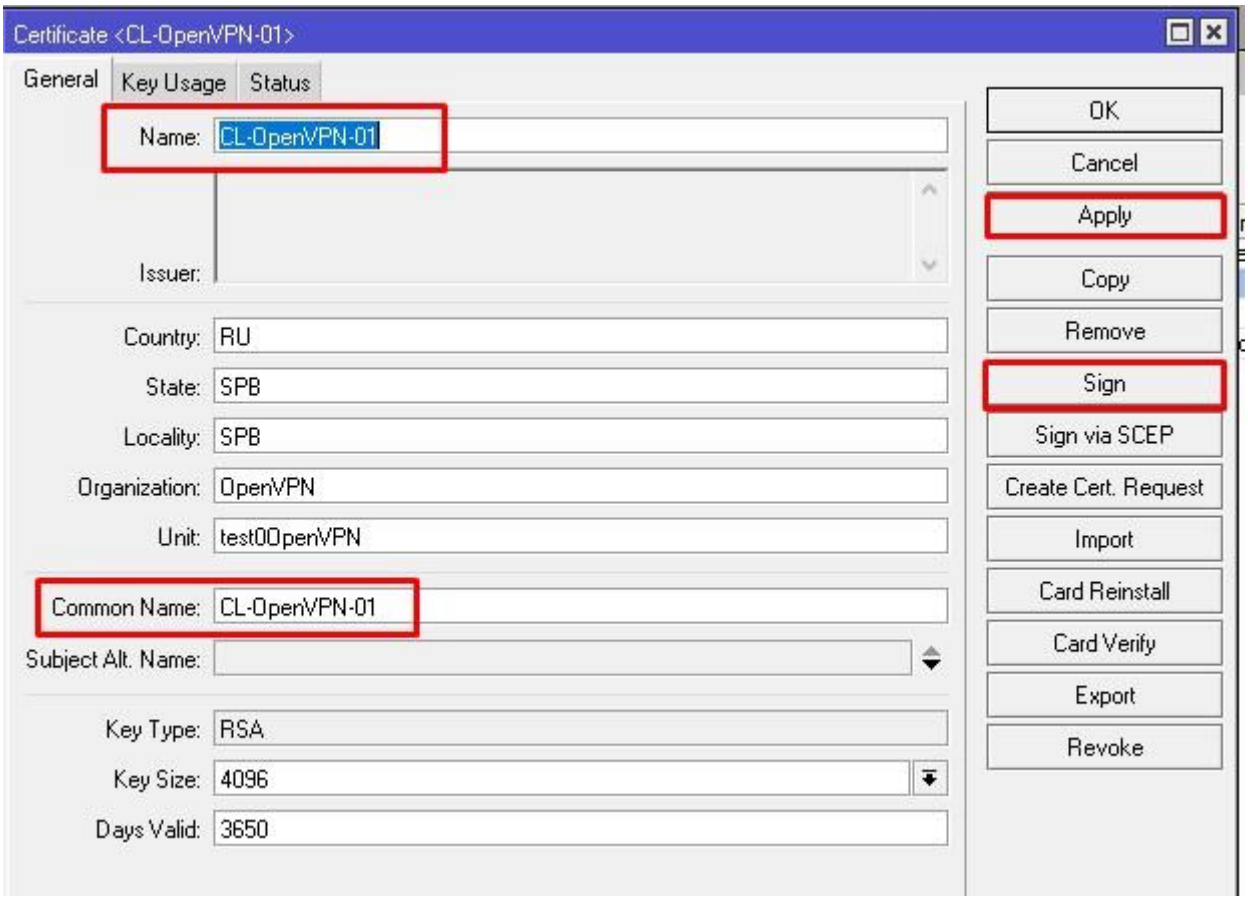
Ping-и идут, а значит с соединением все хорошо.

Настройка OpenVPN по сертификату

Здесь мы рассмотрим как настроить подключение по сертификату, выполним экспортирование и эмпортирование ключей для клиента и сервера.

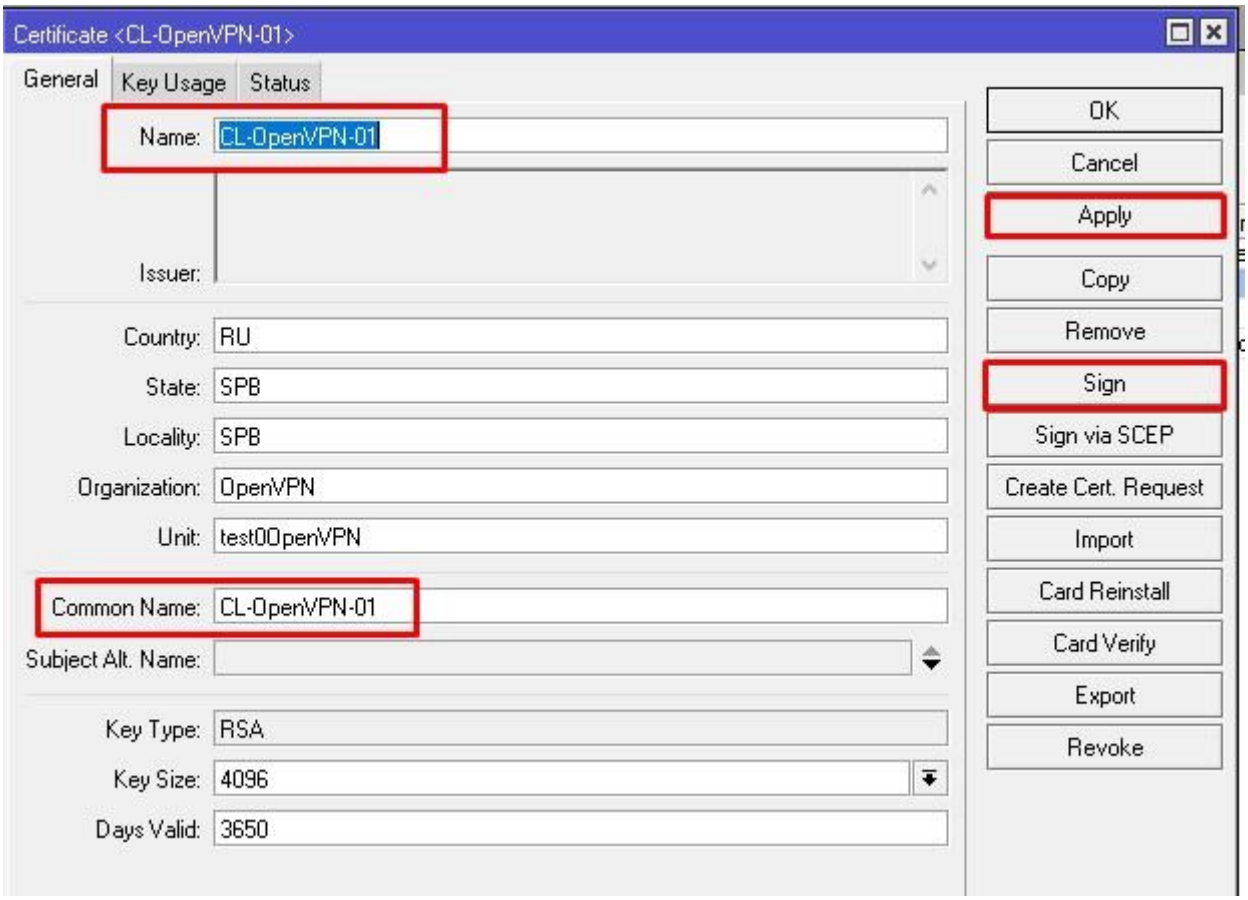
Настройка сервера

Ранее мы настроили аутентификацию по логину и паролю. Настроить аутентификацию только по клиентскому сертификату не получится в связи с ограничением операционной системы. Подключаемся на московский роутер, открываем Certificates и создаем новый шаблон.

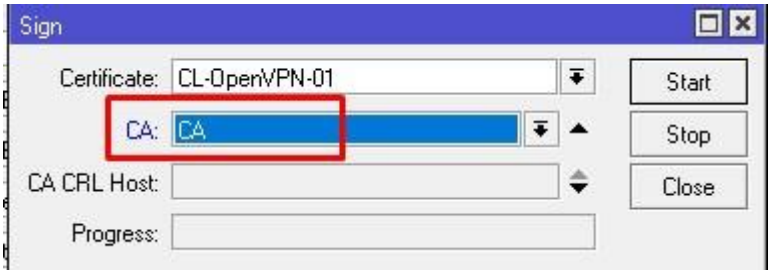


Key Usage. Обязательно ставим галочку на tls client.

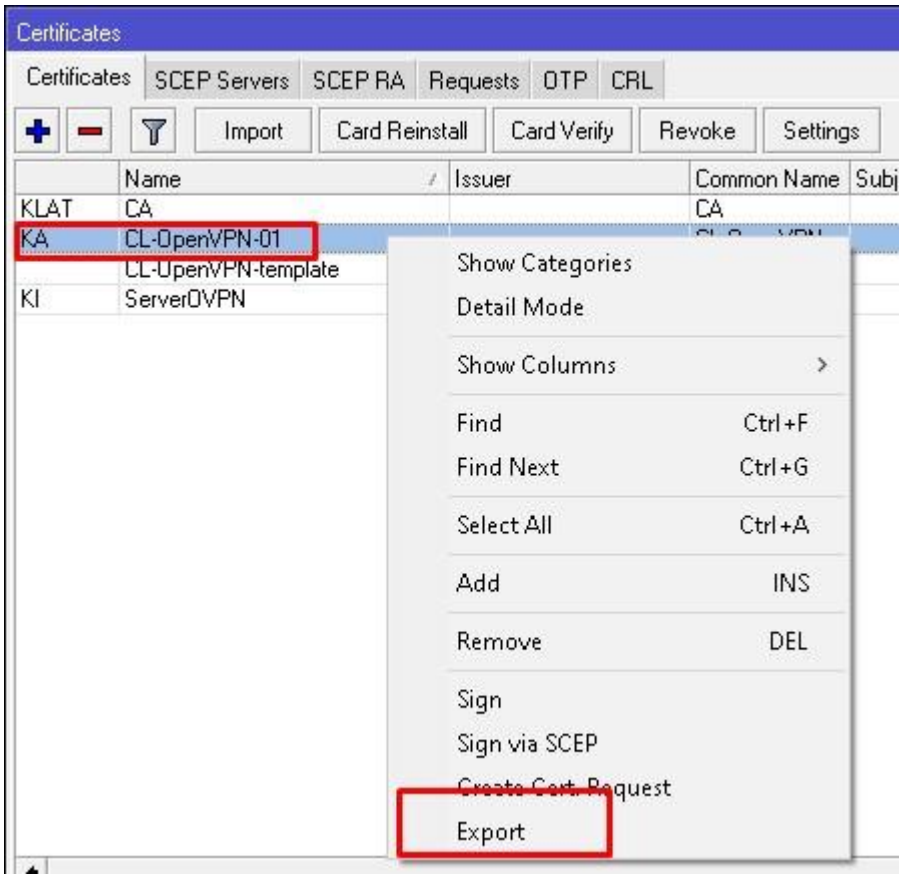
Сохраняем изменения и нажимаем Copy. Выбираем наш шаблон для пользователей и создаём копию. В Common Name уникальное имя. Далее нажимаем Apply и Sign.



В открывшемся окне по аналогии с предыдущих примеров выбираем корневой сертификат и жмем Start.



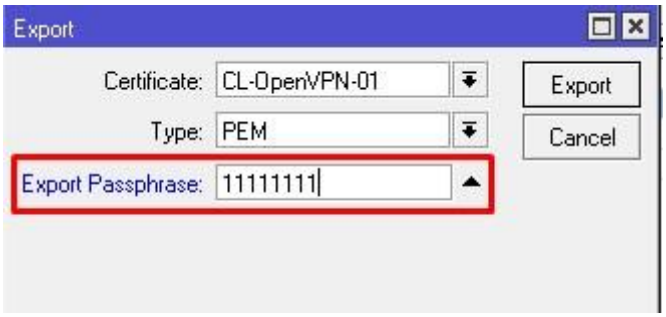
Далее нужно экспортировать и импортировать ключи на клиентский Mikrotik. Выбираем в списке и жмем Export.

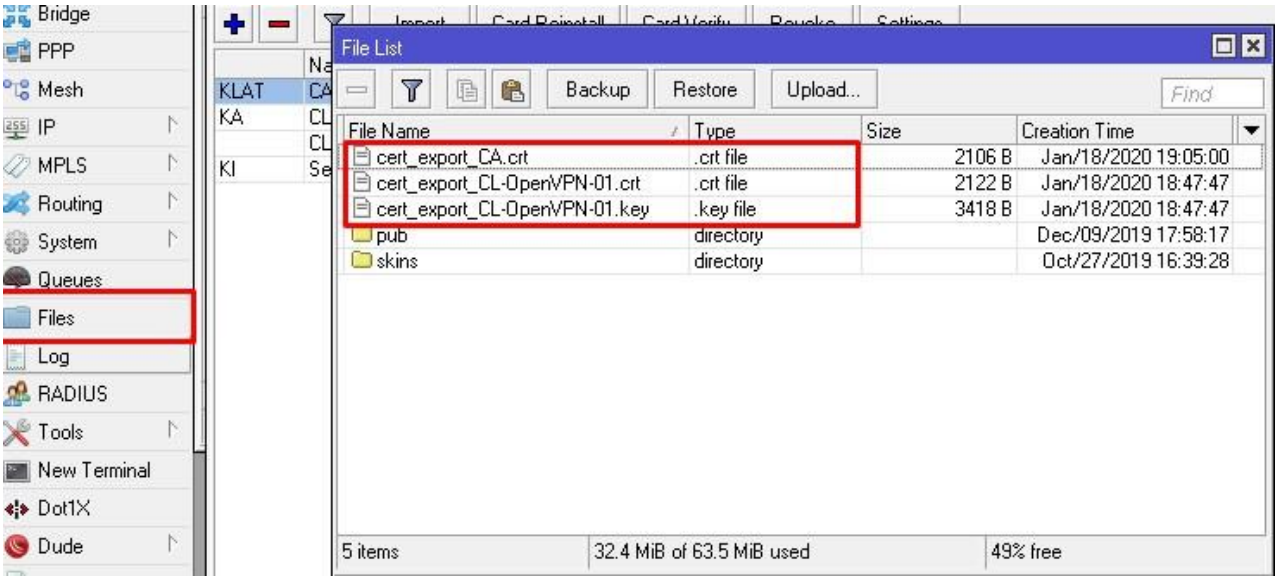


Для того чтобы выгрузить открытый и закрытый ключи, вбиваем пароль в поле Export Passphrase. Export.

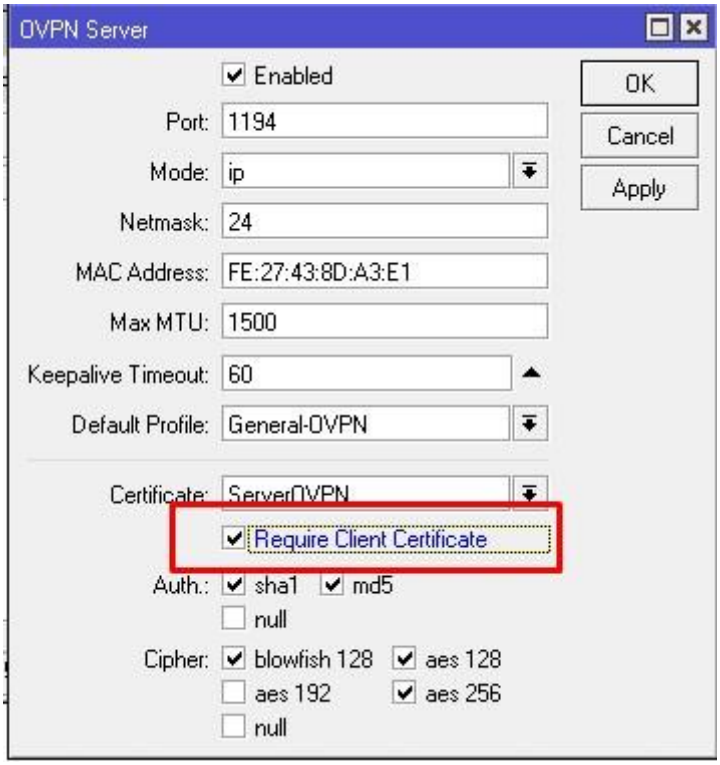
Далее нужно экспортировать открытую часть CA.

Переходим в Files, выбираем 3 созданных файла и перетаскиваем на рабочий стол.



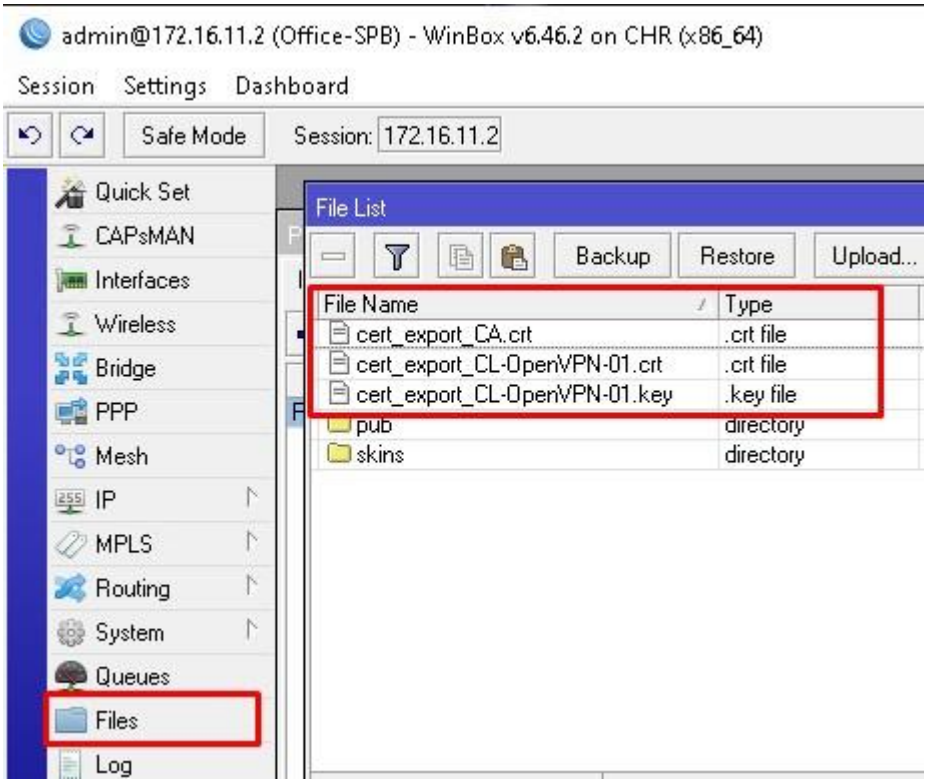


В настройках OVPN Server выставим чтобы проверялись клиентские сертификаты при подключении.



Настройка клиента

После экспорта и копирования ключей подключимся к питерскому роутеру. Открываем Files и переносим с рабочего стола 2 файла скопированных ранее.



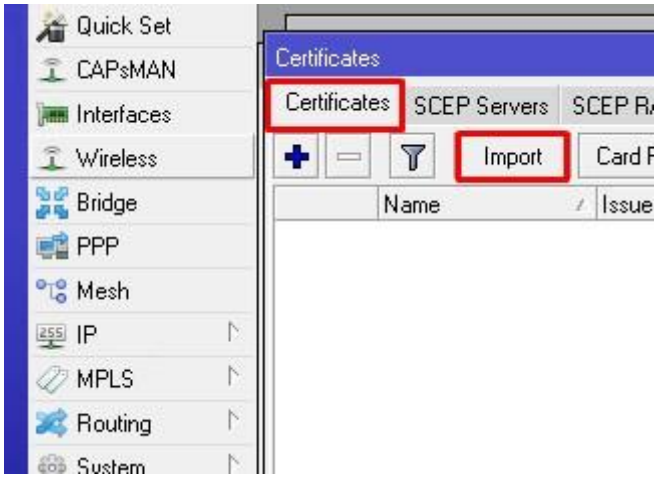
Переходим в Certificates и импортируем открытый и закрытый ключи.

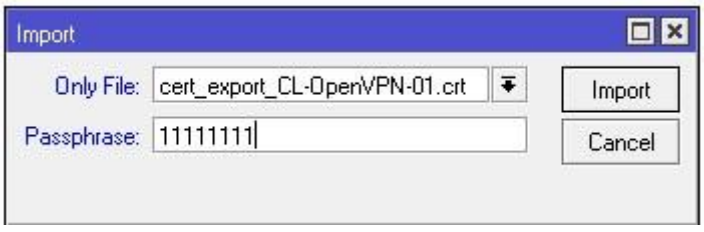
В выпадающем списке выбираем открытый ключ и вписываем пароль. Import.

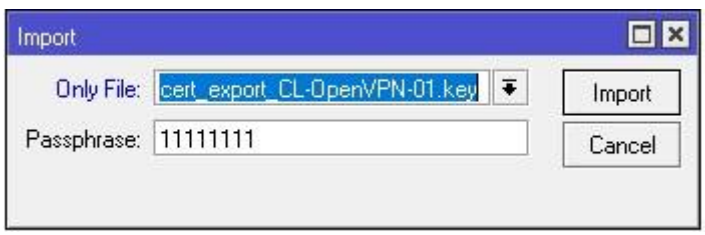
Тоже самое с закрытым ключом.

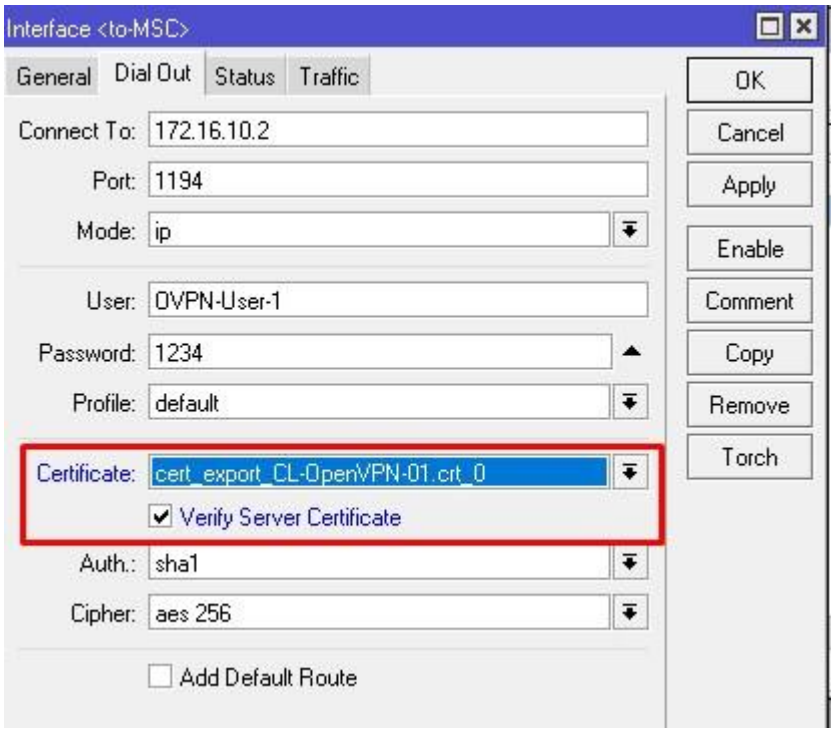
Далее импортируем CA.

Открываем ранее созданный OVPN Client интерфейс, выбираем импортированный сертификат и требуем проверку серверного.

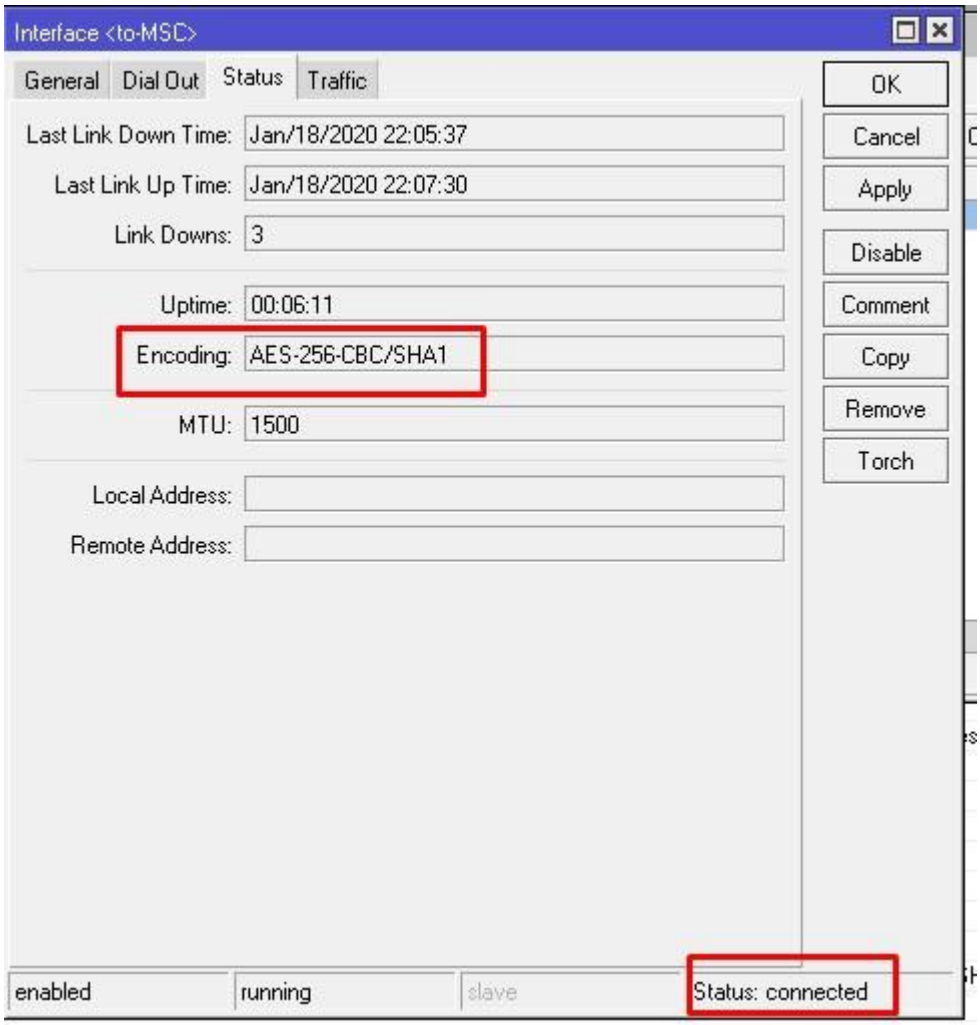








Соединение установилось.

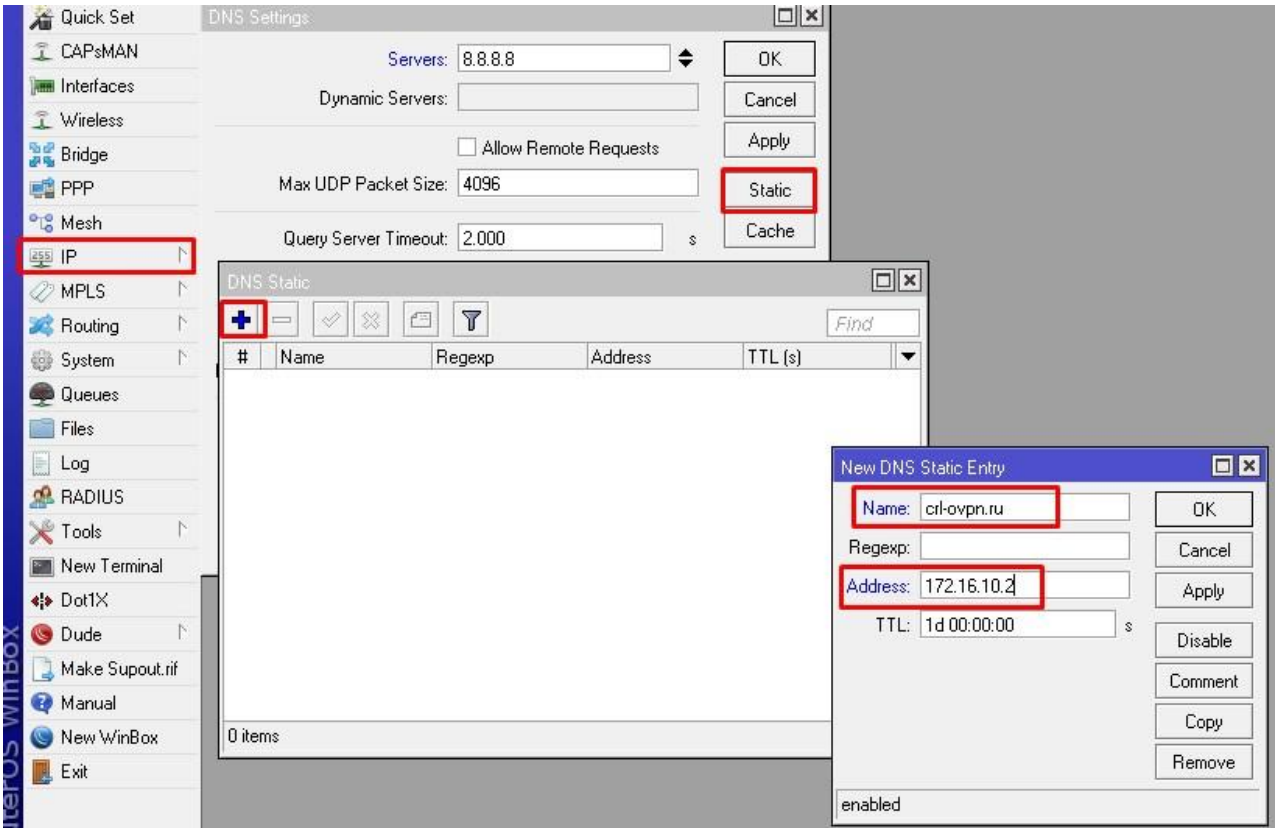


Проверим его.

```
/command        Use command at the base level
[admin@Office-SPB] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    172.16.11.2/24     172.16.11.0     ether1
 1    192.168.10.1/24    192.168.10.0    General-Bridge
 2 D 172.16.25.2/24     172.16.25.0     to-MSC
[admin@Office-SPB] > ping 172.16.25.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 172.16.25.1                                56  64 1ms
    1 172.16.25.1                                56  64 3ms
    2 172.16.25.1                                56  64 1ms
    3 172.16.25.1                                56  64 27ms
    sent=4 received=4 packet-loss=0% min-rtt=1ms avg-rtt=8ms max-rtt=

[admin@Office-SPB] >
```

А вот и не все! Упустили важную вещь – список отзыва. Так как наш клиент использует DNS 8.8.8.8, есть вероятность, что Google понятия не имеет какой IP адрес скрывается за доменным именем crl-ovpn.ru – его мы указывали, когда создавали сертификат для CA. Нужно это быстро исправить. На клиенте в IP – DNS создаем статическую A запись.



На этом все, мы рассмотрели настройку OpenVPN (OVPN) между двумя роутерами микротик, один из них выступал в роли сервера а второй в роли клиента. Если у вас остались вопросы задавайте их в комментариях или нашей группе Телеграмм.

Вы хорошо разбираетесь в Микротиках? Или впервые недавно столкнулись с этим оборудованием и не знаете, с какой стороны к нему подступиться? В обоих случаях вы найдете для себя полезную информацию в углубленном курсе «Администрирование сетевых устройств MikroTik». В курсе много практических лабораторных работ по результату выполнения которых вы получите обратную связь. После окончания обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно тут.