

Настройка OpenVPN-сервера на роутерах Mikrotik. RouterOS 6

 interface31.ru/tech_it/2020/01/nastroyka-openvpn-servera-na-routerah-mikrotik.html

OpenVPN является одной из самых популярных технологий для построения VPN-сетей и это вполне справедливо, данный продукт сочетает в себе безопасность с простой настройкой и мощными возможностями конфигурирования и управления сетью. В роутерах Mikrotik возможности OpenVPN существенно ограничены, что требует серьезно взвесить все за и против перед разворачиванием, тем не менее в ряде случаев настройка OpenVPN выглядит оправданной и сегодня мы расскажем как это сделать.



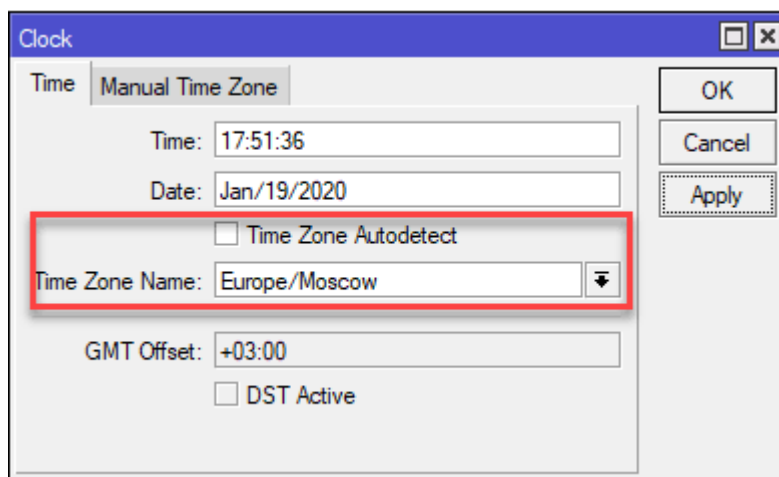
Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на углубленном курсе по администрированию MikroTik. Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

Данная статья предназначена для RouterOS 6.x, для настройки OpenVPN сервера в RouterOS 7.x воспользуйтесь обновленным материалом.

Подготовка роутера

OpenVPN, как и любой другой использующий SSL-шифрование продукт, чувствителен к расхождению времени между клиентом и сервером. Поэтому в первую очередь правильно настроим время на Mikrotik. Прежде всего откроем **System - Clock** и установим правильное значение **часового пояса**, его автоматическое определение лучше отключить.

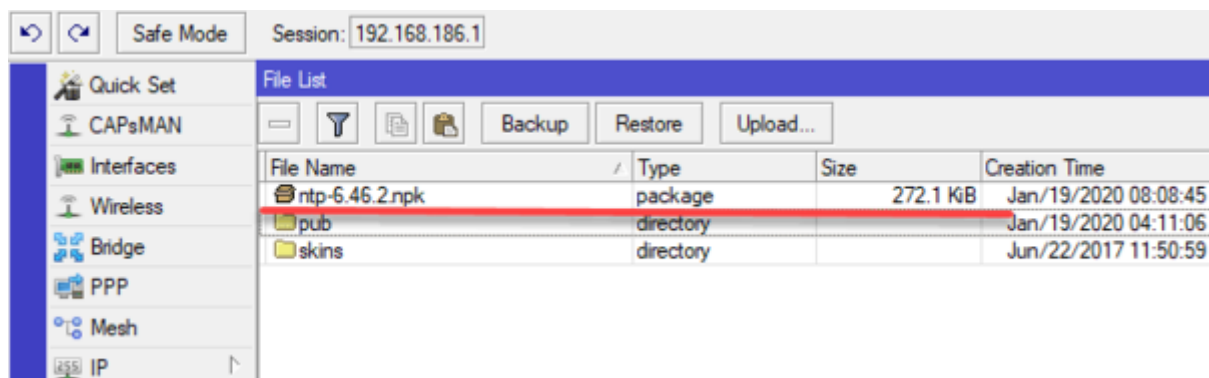


В консоли это можно сделать командой:

```
/system clock  
set time-zone-autodetect=no time-zone-name=Europe/Moscow
```

В качестве параметра опции **time-zone-name** следует указать наименование вашего часового пояса согласно [tz database](#).

Затем установим пакет NTP, для этого вам потребуется скачать с официального сайта архив [Extra packages](#) для вашей архитектуры и версии RouterOS, оттуда следует извлечь пакет **ntp** и поместить его на роутер, для установки достаточно перезагрузить устройство.

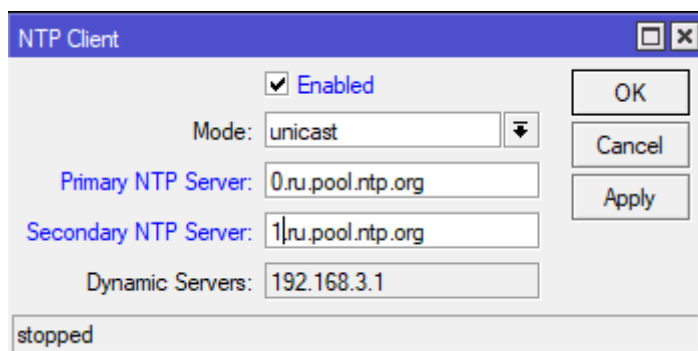


После чего перейдем в **System - NTP Client**, включим его и укажем адреса NTP-серверов, в нашем случае это сервера из пула [ru.pool.ntp.org](#).

В командной строке это можно сделать так:

```
/system ntp client  
set enabled=yes primary-  
ntp=185.209.85.222 secondary-  
ntp=37.139.41.250
```

Обратите внимание, что вместо доменных имен серверов следует указать их IP, имейте ввиду, что адреса **pool.ntp.org** указывают на случайно выбранные из пула сервера, которые меняются каждый час, поэтому полученные вами адреса могут отличаться от указанных нами.



Аналогичные манипуляции следует выполнить на всех роутерах-участниках VPN-сети. Для ПК и других устройств-клиентов также следует настроить синхронизацию времени.

Создание ключей и сертификатов

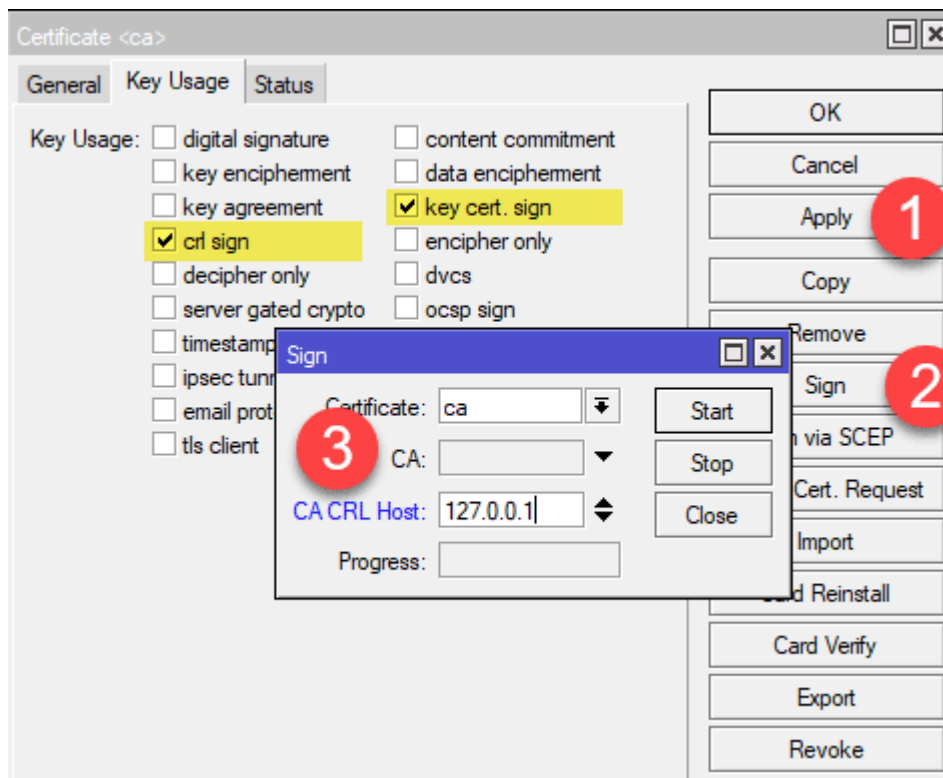
Некоторые руководства в сети предполагают создание ключей и сертификатов при помощи сторонних утилит, например, Easy-RSA, мы же будем использовать собственные средства Mikrotik. Перейдем в **System - Certificate** и создадим новый **корневой сертификат** нашего центра сертификации (CA).

The screenshot shows the 'New Certificate' dialog box with the following details:

- General Tab:**
 - Name:** ca (highlighted with a red box)
 - Issuer:** (empty)
 - Country:** RU
 - State:** 31
 - Locality:** BEL
 - Organization:** Interface LLC
 - Unit:** IT
 - Common Name:** ca (highlighted with a red box)
 - Subject Alt. Name:** (empty)
 - Key Type:** (empty)
 - Key Size:** 2048 (highlighted with a red box)
 - Days Valid:** 3650 (highlighted with a red box)
 - private key:** checked
- Buttons:** OK, Cancel, Apply, Copy, Remove, Sign, Sign via SCEP, Create Cert. Request, Import, Card Reinstall, Card Verify, Export, Revoke.
- Status Bar:** private key, crl, authority, expired, smart card..., trusted.

Обязательные поля отмечены нами красным, это **Name** и **Common Name** - **ca**, размер ключа - **Key Size** - **2048**, и срок действия - **Days Valid** - **3650** или 10 лет, для локального центра сертификации это вполне оправдано. Выделенные зеленым поля содержат информацию о владельце сертификата и к заполнению не обязательны, но их заполнение является правилом хорошего тона и при наличии большого количества сертификатов позволяет быстро понять, что это за сертификат и кому он принадлежит.

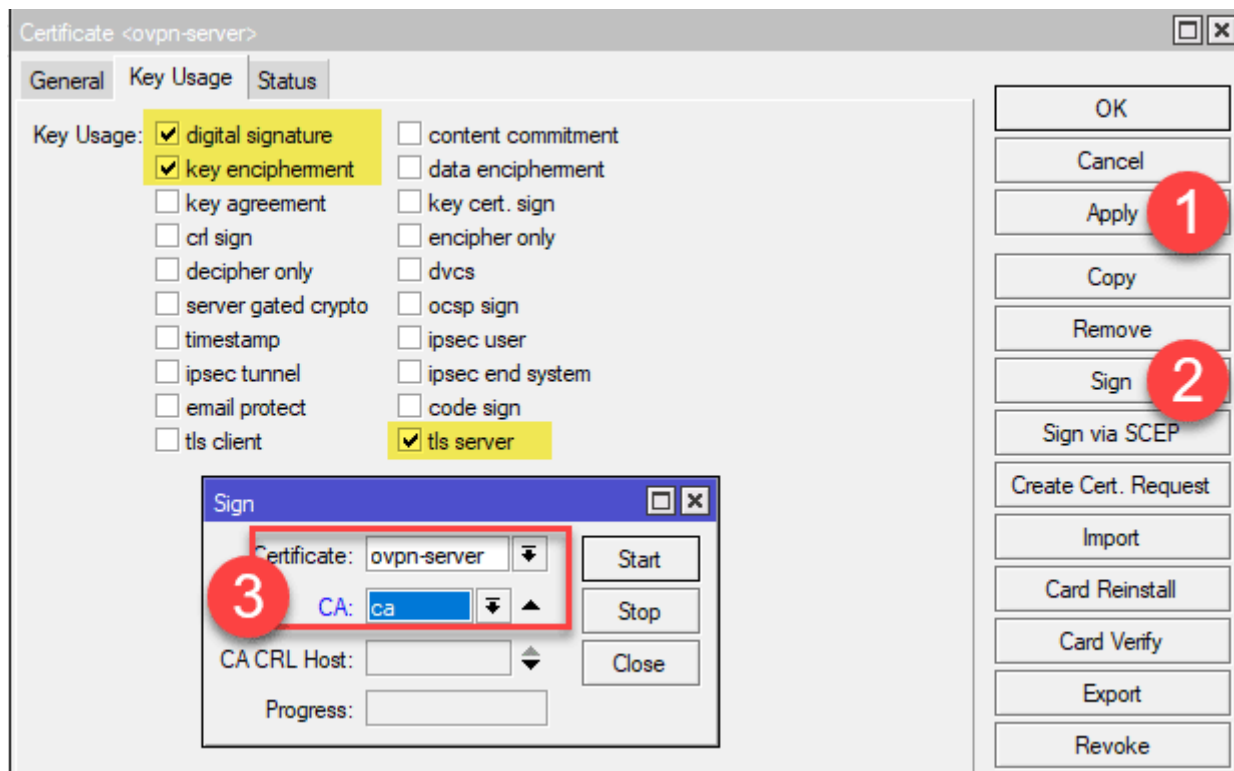
Затем перейдем на закладку **Key Usage** и укажем только **crl sign** и **key cert. sign** и нажмем кнопку **Apply**, теперь подпишем сертификат нажав **Sign**. В появившемся окне заполним поле **CA CRL Host** адресом локальной петли - **127.0.0.1**, после чего нажимаем **Start** и ждем окончания подписи сертификата.



Эти же действия в консоли:

```
/certificate
add name=ca country="RU" state="31" locality="BEL" organization="Interface LLC"
unit="IT" common-name="ca" key-size=2048 days-valid=3650 key-usage=crl-sign,key-
cert-sign
sign ca ca-crl-host=127.0.0.1
```

Следующим создадим сертификат и закрытый ключ сервера. Закладка **General** нового сертификата заполняется аналогично, только в полях **Name** и **Common Name** указываем **ovpn-server** (можете выбрать на собственное усмотрение). На вкладке **Key Usage** укажите **digital-signature**, **key-encipherment** и **tls-server**. Затем подпишем сертификат ключом нашего CA, для этого в поле **CA** выберите только что созданный нами сертификат **ca**.

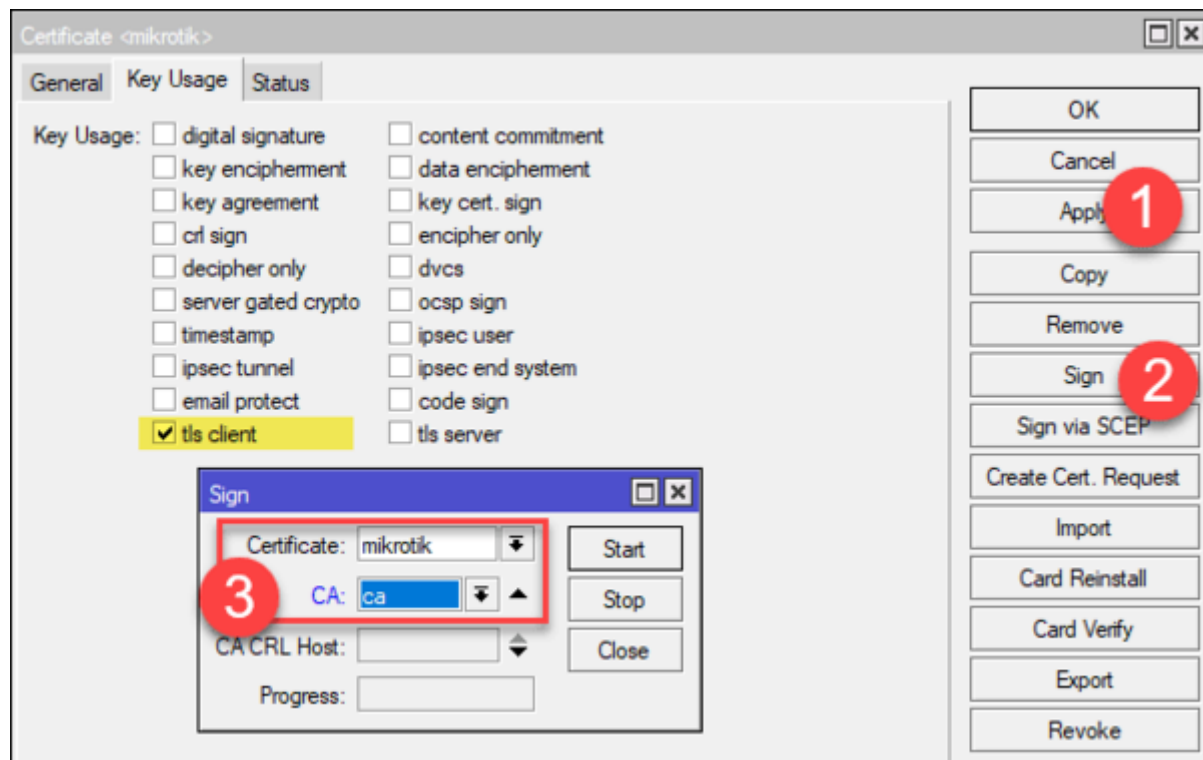


Для выпуска сертификата в консоли выполните:

```
/certificate
add name=ovpn-server country="RU" state="31" locality="BEL"
organization="Interface LLC" unit="IT" common-name="ovpn-server" key-size=2048
days-valid=3650 key-usage=digital-signature,key-encipherment,tls-server
sign ovpn-server ca="ca"
```

Теперь создадим клиентские сертификаты, в полях **Name** и **Common Name** на закладке **General** указываем имя сертификата, его следует давать осмысленно, чтобы всегда можно было определить какому клиенту принадлежит сертификат. Также следует подумать над **сроком действия сертификата**, если клиентом будет роутер в удаленном офисе, то можно также выпустить сертификат на 10 лет, а вот если клиентом будет ноутбук сотрудника на испытательном сроке, то лучше выдать его на срок испытательного срока. Выпустить новый сертификат не представляет проблемы, в то время как не отзыванный вовремя сертификат может привести к несанкционированному доступу и утечке данных.

На вкладке **Key Usage** указываем только **tls-client** и также подписываем сертификат ключом нашего CA. Можно сразу выпустить все необходимые клиентские сертификаты, можно создавать их по мере необходимости.



Получение клиентского сертификата в консоли:

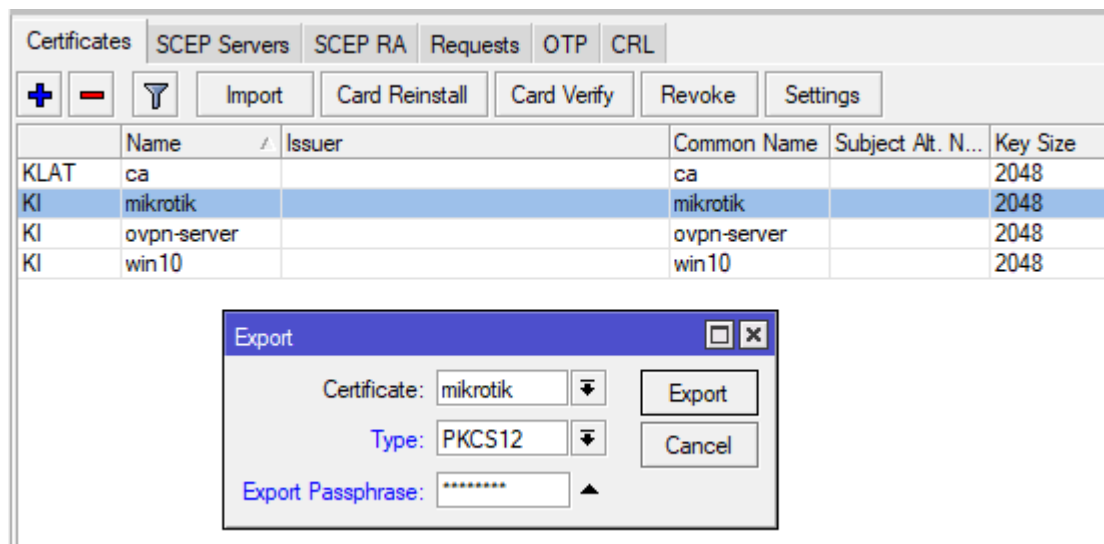
```
/certificate
add name=mikrotik country="RU" state="31" locality="BEL" organization="Interface
LLC" unit="IT" common-name="mikrotik" key-size=2048 days-valid=365 key-usage=tls-
client
sign mikrotik ca="ca"
```

Обратите внимание, в данном случае мы выпустили сертификат со сроком действия в 1 год: **days-valid=365**.

Если все сделано правильно, то у вас будут следующие сертификаты, обратите внимание, что корневой сертификат должен иметь флаги KLAT, остальные KI:

Certificates									
Certificates SCEP Servers SCEP RA Requests OTP CRL									
+ - Import Card Reinstall Card Verify Revoke Settings									
	Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL	CA
KLAT	ca		ca		2048	3650	yes		
KI	mikrotik		mikrotik		2048	365	no		ca
KI	ovpn-server		ovpn-server		2048	3650	no		ca
KI	win10		win10		2048	365	no		ca

Для использования на клиента нам необходимо экспортировать закрытый ключ и сертификат клиента, а также корневой сертификат центра сертификации. Удобнее всего использовать для этого формат PKCS12, который содержит все необходимые компоненты в одном файле (сертификат, ключ и сертификат CA). Для этого щелкните на нужном сертификате правой кнопкой и выберите **Export**, в открывшемся окне укажите формат **Type - PKCS12** и парольную фразу для экспорта (минимум 8 символов) в поле **Export Passphrase**. Без указания пароля закрытые ключи выгружены не будут, и вы не сможете использовать такой сертификат для клиента.



Либо используйте команды:

```
/certificate
export-certificate mikrotik type=pkcs12 export-passphrase=12345678
```

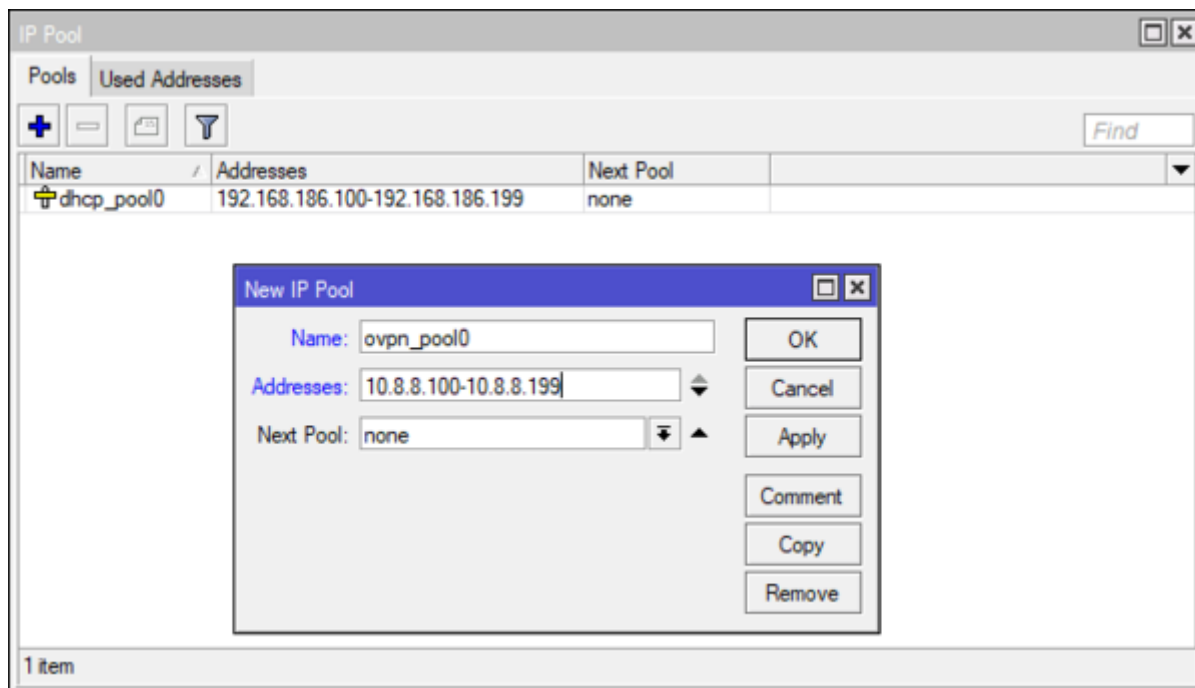
В данном случае мы использовали парольную фразу **12345678**. Экспортированные сертификаты можно скачать в разделе **Files**.

File List				
<div> <div> <div></div> <div></div> <div></div> </div> <div>Backup</div> <div>Restore</div> <div>Upload...</div> </div>				
File Name	Type	Size	Creation Time	
autosupout.old.rif	.rif file	654.9 KiB	Nov/04/2019 16:55:30	
autosupout.rif	.rif file	682.1 KiB	Nov/04/2019 17:05:19	
cert_export_mikrotik.p12	p12 file	2228 B	Jan/19/2020 01:33:05	
cert_export_win10.p12	p12 file	2220 B	Jan/19/2020 01:33:11	
lists.rsc	script	5.6 KiB	Nov/04/2019 20:59:36	
pub	directory		Jul/08/2019 06:34:37	
skins	directory		Jun/22/2017 11:50:59	

Как видим, возможности RouterOS легко позволяют управлять сертификатами без привлечения дополнительных инструментов.

Настройка OpenVPN сервера

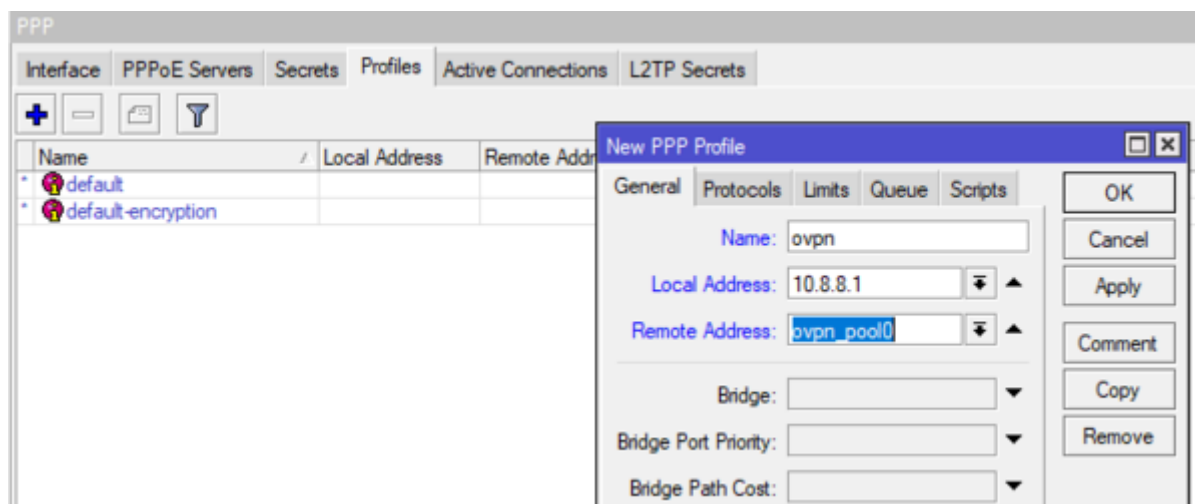
Начнем с создания пула адресов для выдачи OpenVPN клиентам, так как назначать адреса вручную во втором десятилетии 21 века - дурной тон. Для этого перейдем в **IP - Pool** и создадим новый пул: **Name** - **ovpn_pool0** - произвольное имя пула, **Addresses** - **10.8.8.100-10.8.8.199** - диапазон адресов для выдачи клиентов, также можете выбрать по собственному усмотрению.



Эти же действия в консоли:

```
/ip pool
add name=ovpn_pool0 ranges=10.8.8.100-10.8.8.199
```

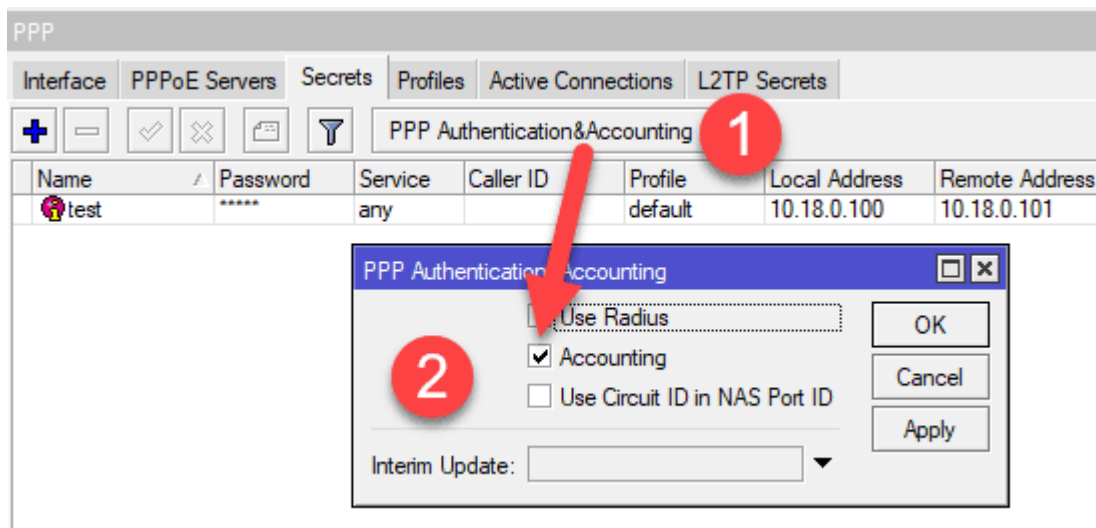
Теперь перейдем в **PPP - Profiles** и создадим новый профиль. Укажем его имя **Name - ovpn**, локальный и удаленный адреса: **Local Address - 10.8.8.1**, **Remote Address - ovpn_pool0**. На всякий случай напомним, что локальный адрес должен принадлежать той-же /24 сети, что и диапазон пула адресов.



Быстро создать профиль в терминале:

```
/ppp profile
add local-address=10.8.8.1 name=ovpn remote-address=ovpn_pool0
```

Затем перейдем в **PPP - Secrets** и убедимся, что включена аутентификация по пользователю. Для этого нажмем **PPP Authentication&Accounting**, где должен стоять флаг **Accounting**:



Хотя гораздо быстрее выполнить команду:

```
/ppp aaa
set accounting=yes
```

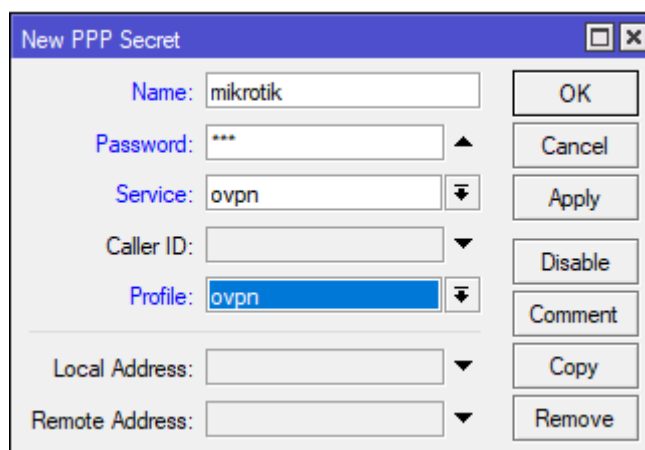
Здесь же создадим учетные записи для клиентов. Особенностью реализации OpenVPN в RouterOS 6 является обязательное использование аутентификации по имени и паролю. При создании учетной записи указываем ее имя - **Name**, рекомендуем дать ей то же самое имя, которое вы использовали при создании сертификата, чтобы избежать путаницы. **Password** - пароль, так как основная аутентификация производится по сертификату особых требований к нему нет. **Service** - какие службы могут использовать данную учетную запись - ограничиваем только OpenVPN выбрав **ovpn**, затем указываем созданный нами профиль **Profile** - **ovpn**.

В терминале для создания учетной записи выполните:

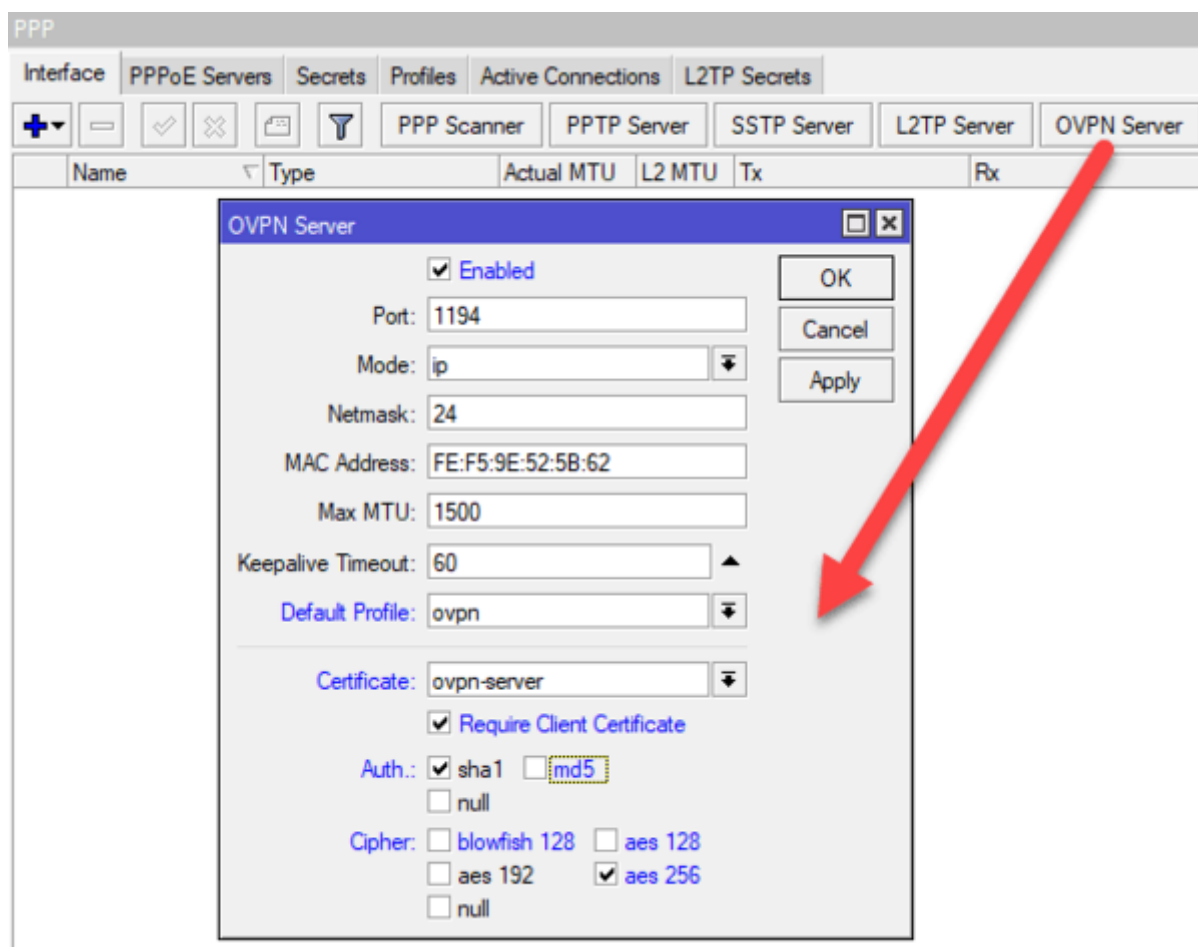
```
/ppp secret
add name=mikrotik password=123
profile=ovpn service=ovpn
```

В данном случае мы создали запись для пользователя **mikrotik** с паролем **123**.

После создания пользователей перейдем в **PPP - Interface** и нажмем на кнопку **OVPN Server**, в открывшемся окне включим службу установив флаг **Enabled**, **Default Profile** - **ovpn**, в поле **Certificate** укажем созданный нами сертификат сервера. Для дополнительной безопасности включим **Require Client Certificate**, в этом случае сервер будет проверять сертификат клиента на принадлежность к цепочке сертификатов локального CA. Затем укажем параметры шифрования: **Auth** - безальтернативно **sha1**, **Cipher** - здесь есть возможность



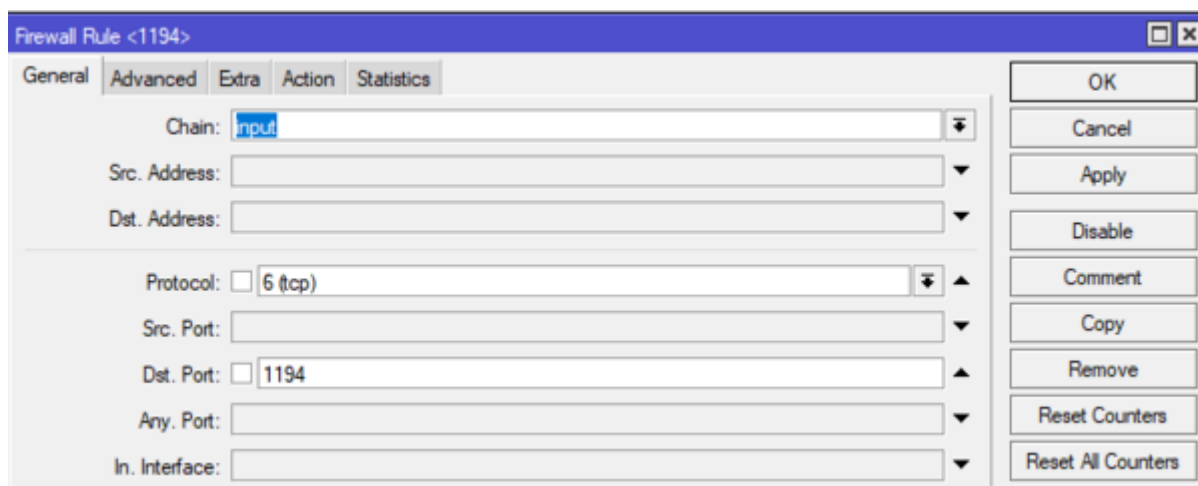
выбора, для роутеров с аппаратной поддержкой AES следует выбирать шифры только из этого семейства, однако чем сильнее шифр - тем больше он нагружает оборудование.



В терминале эти же действия выполняются командами:

```
/interface ovpn-server server
set auth=sha1 certificate=ovpn-server cipher=aes256 default-profile=ovpn
enabled=yes require-client-certificate=yes
```

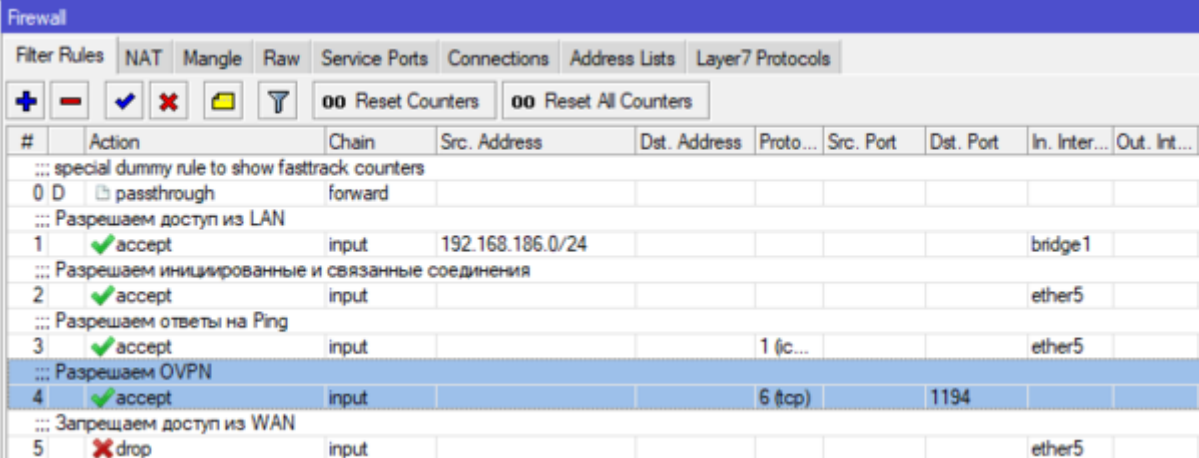
Также не забудьте разрешить входящие подключения к вашему OpenVPN серверу. Откроем **IP - Firewall** и добавим правило: **Chain - input, Protocol - tcp, Dst. Port - 1194**. Действие можно не указывать, так как по умолчанию применяется **accept**.



В терминале выполните:

```
/ip firewall filter
add action=accept chain=input dst-port=1194 protocol=tcp
```

Данное правило должно располагаться выше запрещающего в цепочке INPUT.

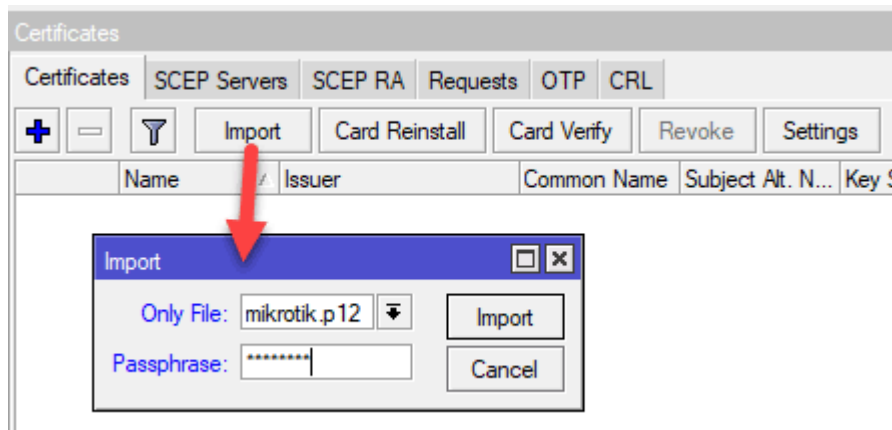


#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...
0	passthrough	forward							
1	accept	input	192.168.186.0/24					bridge1	
2	accept	input						ether5	
3	accept	input			1 (ic...			ether5	
4	accept	input			6 (tcp)		1194		
5	drop	input						ether5	

На этом настройка OpenVPN сервера на базе роутера Mikrotik закончена.

Настройка OpenVPN клиента на роутере Mikrotik

Прежде всего закачаем на устройство файл сертификатов в формате PKCS12, который мы экспортировали на сервере. Для этого перейдем в **System - Certificate** и воспользуемся кнопкой **Import**, в открывшемся окне укажем **файл сертификата** и **парольную фразу**, которую мы установили при экспорте.



В консоли выполните:

```
/certificate
import file-name=mikrotik.p12 passphrase=12345678
```

В результате у вас появятся два сертификата: сертификат клиента с закрытым ключом, о чем говорит флаг КТ, и корневой сертификат удостоверяющего центра с флагом LAT (К - означает наличие ключа). Запомним наименование сертификатов, либо переименуем их.

Certificates					
Certificates SCEP Servers SCEP RA Requests OTP CRL					
Import Card Reinstall Card Verify Revoke Settings					
	Name /	Issuer	Common Name	Subject Alt. N...	Key Size
KT	mikrotik.p12_0	C=RU,ST=31,L=BEL,O=Interface LLC,OU=IT,CN=ca	mikrotik		2048
LAT	mikrotik.p12_1	C=RU,ST=31,L=BEL,O=Interface LLC,OU=IT,CN=ca	ca		2048

Затем перейдем в **PPP - Interface** и создадим новый интерфейс типа **OVPN Client**. В поле **Connect To** указываем адрес или FQDN-имя вашего OpenVPN сервера, **Port - 1194**, **Mode - ip**. Ниже указываем учетные данные, созданные для этого пользователя на сервере в полях **User** и **Password**, еще ниже указываем параметры шифрования: **Auth - sha1**, **Cipher** - аналогично тому, что вы указали на сервере. В поле **Certificate** выберите сертификат клиента, флаг **Verify Server Certificate** следует снять.

В терминале следует выполнить:

```
/interface ovpn-client
add certificate=mikrotik.p12_0 cipher=aes256 connect-to=192.168.3.115 name=ovpn-out1 password=123 user=mikrotik
```

Если все было сделано правильно, то соединение будет установлено сразу как вы создадите интерфейс.

Чтобы клиенты сети за клиентом имели доступ в сеть за сервером и наоборот необходимо настроить маршрутизацию. Перейдем в **IP - Routes** и добавим новый маршрут. В поле **Dst. Address** укажем сеть за сервером, в нашем случае это **192.168.186.0/24**, в поле **Gateway** укажем интерфейс нашего OpenVPN подключения - **ovpn-out1**.

New Route

General | Attributes

Dst. Address: 192.168.186.0/24

Gateway: ovpn-out1

Check Gateway:

Type: unicast

Distance:

Scope: 30

Target Scope: 10

Либо выполните команду:

```
/ip route
add distance=1 dst-address=192.168.186.0/24 gateway=ovpn-out1
```

Теперь перейдем на сервер и посмотрим каким образом выглядит подключение данного клиента. Как видим, был создан динамический интерфейс **ovpn-mikrotik**, настраивать маршрутизацию с таким интерфейсом нельзя, так как маршрут "сломается" при отключении клиента.

Interface List

Interface | Interface List | Ethernet | EoIP Tunnel | IP Tunnel | GRE Tunnel | VLAN | VRRP | Bonding | LTE

+ - [] [X] [] [] [] Detect Internet

	Name /	Type	Actual MTU	L2 MTU	Tx	Rx
DR	<><ovpn-mikrotik>	OVPN Server Binding	1500		0 bps	0 bps
... LAN						
R	bridge1	Bridge	1500	65535	42.3 kbps	2.2 kbps
... LAN						
RS	ether1	Ethernet	1500		42.7 kbps	2.6 kbps
XS	ether2	Ethernet	1500		0 bps	0 bps
XS	ether3	Ethernet	1500		0 bps	0 bps
XS	ether4	Ethernet	1500		0 bps	0 bps
... WAN						
R	ether5	Ethernet	1500		0 bps	14.4 kbps

Поэтому создадим для этого клиента постоянный интерфейс. Перейдем в **Interfaces** и создадим новый интерфейс типа **OVPN Server Binding**. В настройках укажем имя, рекомендуется давать интерфейсам понятные имена, **Name - ovpn-mikrotik**, в поле **User** - укажем пользователя, подключение которого будет привязано к этому интерфейсу - **mikrotik**.

Это же можно сделать командой:

```
/interface ovpn-server
add name=ovpn-mikrotik user=mikrotik
```

После чего можно добавить на сервере маршрут к сети за клиентом, настройки здесь аналогичные, **Dst. Address** - сеть за клиентом, **Gateway** - интерфейс OpenVPN подключения. В нашем случае **192.168.111.0/24** - сеть за клиентом.

В терминале следует выполнить:

```
/ip route
add distance=1 dst-address=192.168.111.0/24 gateway=ovpn-mikrotik
```

После чего можем проверить связь. Узлы различных сетей должны видеть друг друга.

Настройка стандартного клиента OpenVPN на ПК

Немного изменим задачу, будем считать, что у нас есть ноутбук сотрудника с установленным клиентом OpenVPN, которому необходимо обеспечить доступ в корпоративную сеть через OpenVPN сервер на роутере Mikrotik. Будем считать, что OpenVPN установлен в **C:\OpenVPN**, а для хранения ключей используется директория **C:\OpenVPN\keys**.

Прежде всего разместим файл сертификатов в формате PKCS12 в директории для хранения ключей, а также создадим файл с учетными данными

C:\OpenVPN\auth.cfg и разместим в нем в разных строках логин и пароль:

```
win10  
123
```

Где win10 - имя пользователя, 123 - пароль которые мы задали для этой учетной записи на сервере.

Теперь создадим файл **C:\OpenVPN\keypass.cfg** в котором разместим парольную фразу для сертификата:

```
12345678
```

За основу конфигурационного файла мы примем стандартный шаблон **client.ovpn**, который расположен в **C:\OpenVPN\sample-config**. Его следует скопировать в **C:\OpenVPN\config**, ниже будут приведены только ключевые опции, а также те, которые мы изменяем или добавляем.

Укажем, что у это клиент, тип туннеля - tun и протокол tcp:

```
client  
dev tun  
proto tcp
```

Адрес и порт сервера:

```
remote 192.168.3.115 1194
```

Убедимся в наличии опций:

```
persist-key  
persist-tun
```

Затем заменим весь блок с указанием путей к ключам и сертификатам:

```
ca ca.crt  
cert client.crt  
key client.key
```

единственной строкой:

```
pkcs12 C:\\OpenVPN\\keys\\win10.p12
```

где укажем путь к нашему файлу сертификатов в формате PKCS12.

Ниже добавим две строки с указанием, где брать учетные данные для дополнительной аутентификации и парольную фразу:

```
auth-user-pass C:\\OpenVPN\\auth.cfg  
askpass C:\\OpenVPN\\keypass.cfg
```

Проверим наличие опции:

```
remote-cert-tls server
```

и прокомментируем:

```
#tls-auth ta.key 1
```

Сразу добавим маршрут к сети за сервером:

```
route 192.168.186.0 255.255.255.0 10.8.8.1
```

Укажем выбранный нами на сервере шифр:

```
cipher AES-256-CBC
```

и отключим сжатие:

```
#comp-lzo
```

Теперь можно пробовать подключаться. Если все сделано правильно, то клиент подключится к серверу и ему будут доступны ресурсы сети за сервером. Никаких дополнительных настроек на сервере производить не нужно.

Если за данным ПК у вас находится сеть и нужно обеспечить связь между сетями, то нужно выполнить настройки на сервере аналогичные предыдущей части: создать интерфейс для подключения клиента и добавить маршрут для сети за клиентом. На клиентском ПК не забудьте включить службу маршрутизации.

Данная инструкция также полностью подходит для ПК на Linux, вам потребуется только откорректировать пути в конфигурационном файле и раскомментировать в нем опции:

```
user nobody  
group nogroup
```

Как видим, настройка OpenVPN сервера на роутерах Mikrotik достаточно проста, но требует учитывать особенности и ограничения реализации этой технологии в RouterOS.

Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.