

Настройка OpenVPN Сервера и Клиента на MikroTik

mikrotiklab.ru/nastrojka/artga-openvpn.html

January 20, 2020

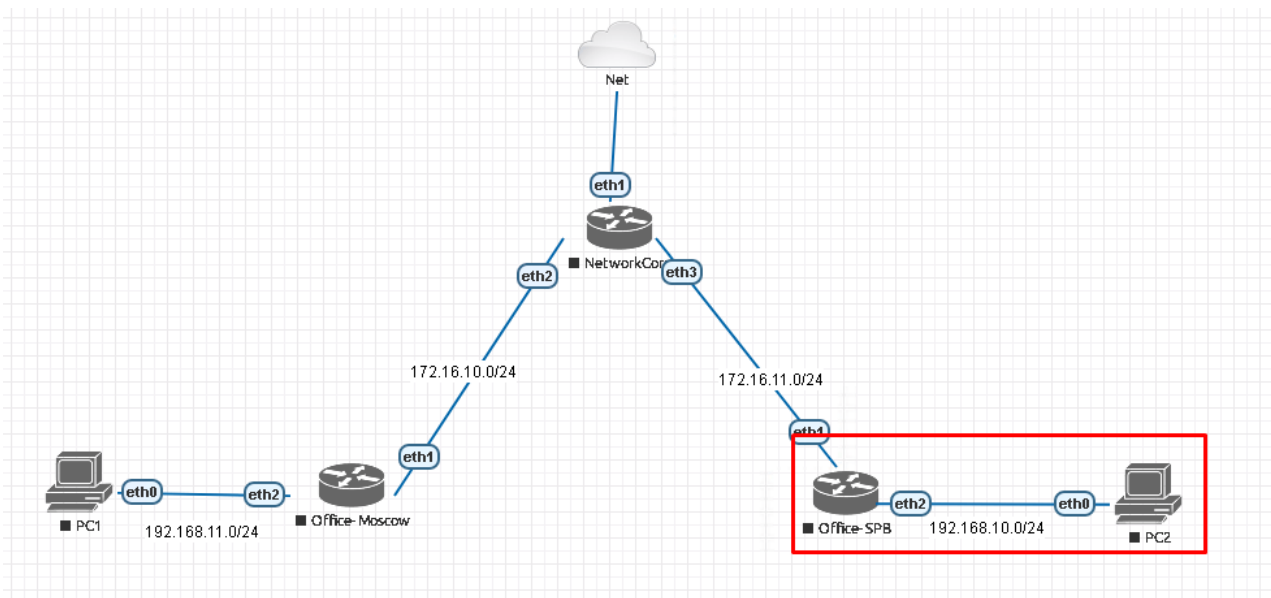
В данной инструкции я покажу настройку между двумя Mikrotik OpenVPN Server и Client. Будем делать аутентификацию без сертификата и с ним. Конфигурация с сертификатами требует большой подготовки и ответственности, так как нам нужно всегда думать о сохранности, актуальности и списке отзыва, но не оспоримый плюс — это высокая безопасность. Правилom 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.

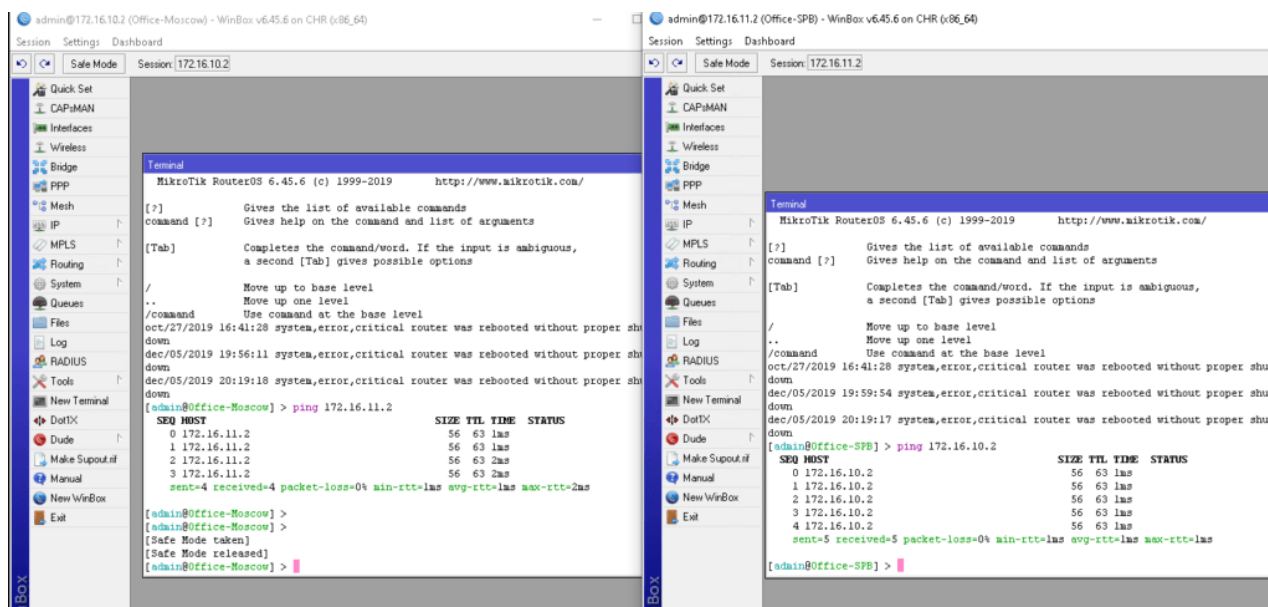
Наша команда рекомендует изучить Наша команда рекомендует изучить углубленный курс по администрированию сетевых устройств MikroTik В курсе много лабораторных работ по итогам которых вы получите обратную связь. После обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно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

Содержание

1. Настройка OpenVPN по логину и паролю
2. Создание сертификата центра сертификации
3. Создание сертификата сервера OpenVPN
4. Конфигурирование сервера
5. Настройка Firewall
6. Конфигурирование клиента
7. Настройка OpenVPN по сертификату
8. Настройка сервера
9. Настройка клиента

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.



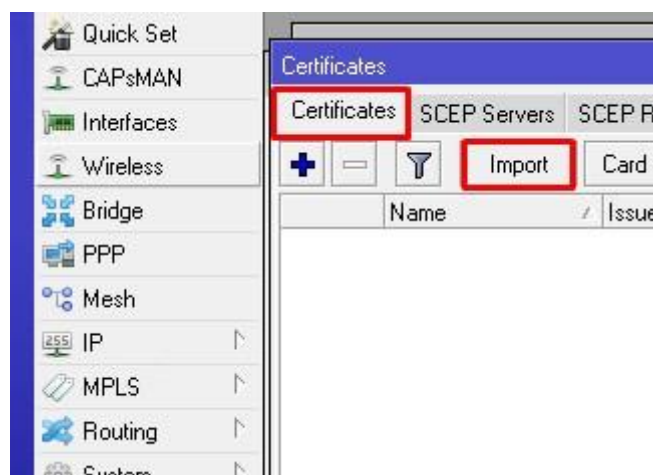
Создание сертификата центра сертификации

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, State, 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.

Certificates: S

General Key Usage Status

Name: CA

Issuer:

Country: RU

State: Moscow

Locality: Moscow

Organization: OpenVPN

Unit: test-OpenVPN

Common Name: CA

Subject Alt. Name:

Key Type:

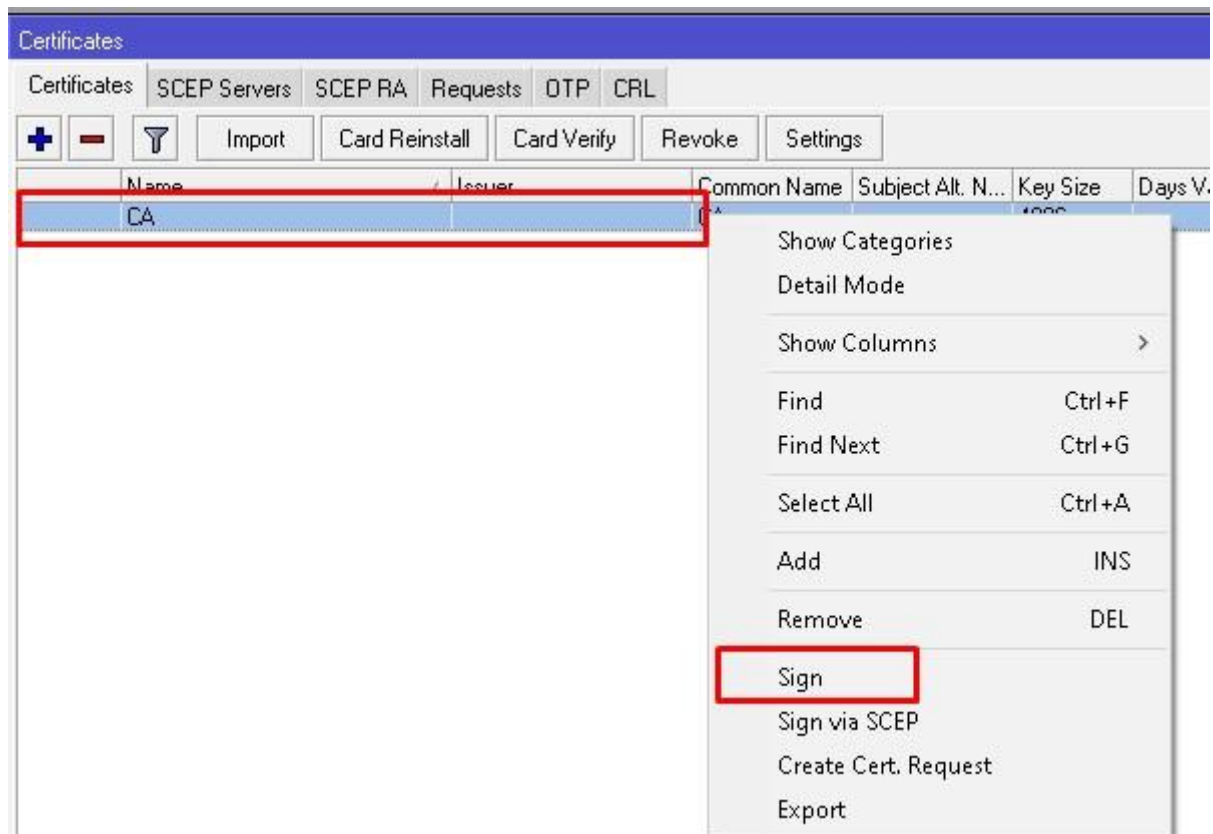
Key Size: 4096

Days Valid: 3650

На данный момент мы создали шаблон.

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

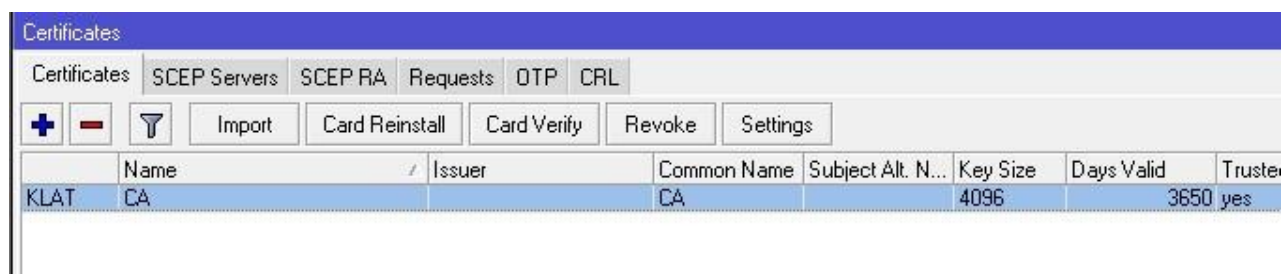
Ничего страшного в этом нет, т.к. мы не собираемся его использовать для других сервисов. Выбираем наш шаблон, и в контекстном меню выбираем Sign.



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.

New Certificate

General | Key Usage | Status

Name: ServerOVPN

Issuer:

Country: RU
State: Moscow
Locality: Moscow
Organization: OpenVPN
Unit: test00penVPN

Common Name: ServerOVPN

Subject Alt. Name:

Key Type: private key
Key Size: 4096
Days Valid: 3650

OK
Cancel
Apply
Copy
Remove
Sign
Sign via SCEP
Create Cert. Request
Import
Card Reinstall
Card Verify
Export
Revoke

Открываем Key Usage, снимаем галочки с:

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

Сохраняем. Переходим к подписанию.

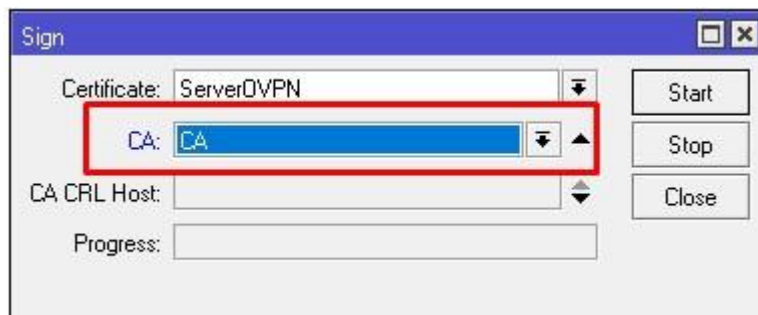
Выбираем сертификат в списке. В контекстном меню нам нужен Sign. В Certificate выбираем шаблон ServerOVPN, в CA самоподписанный корневой сертификат. Start.

New Certificate

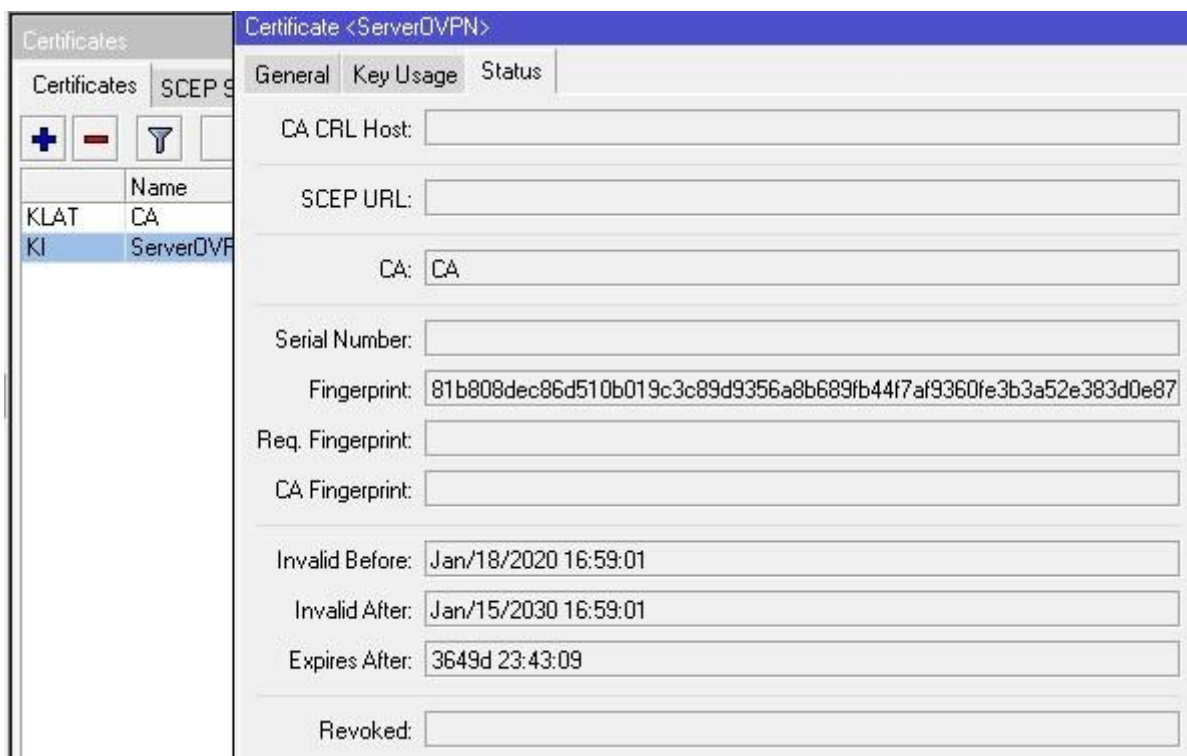
General | Key Usage | Status

Key Usage:

- ☒ digital signature
- ☒ key encipherment
- ☐ key agreement
- ☐ crl sign
- ☐ decipher only
- ☐ server gated crypto
- ☐ timestamp
- ☐ ipsec tunnel
- ☐ email protect
- ☐ tls client
- ☐ content commitment
- ☐ data encipherment
- ☐ key cert. sign
- ☐ encipher only
- ☐ dvcs
- ☐ ocsp sign
- ☐ ipsec user
- ☐ ipsec end system
- ☐ code sign
- ☒ tls server

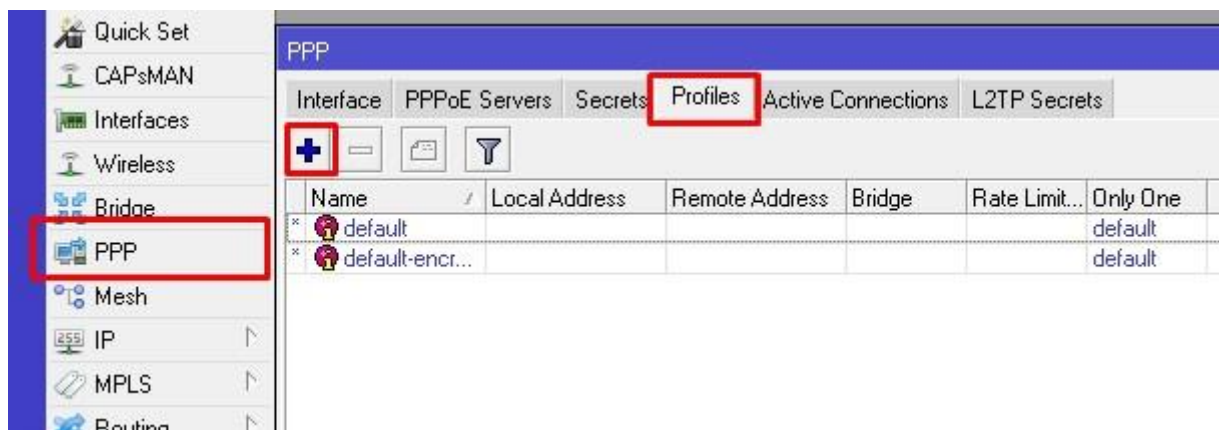


В списке видим, что наш шаблон превратился в полноценный сертификат. Можем открыть его свойства.



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:

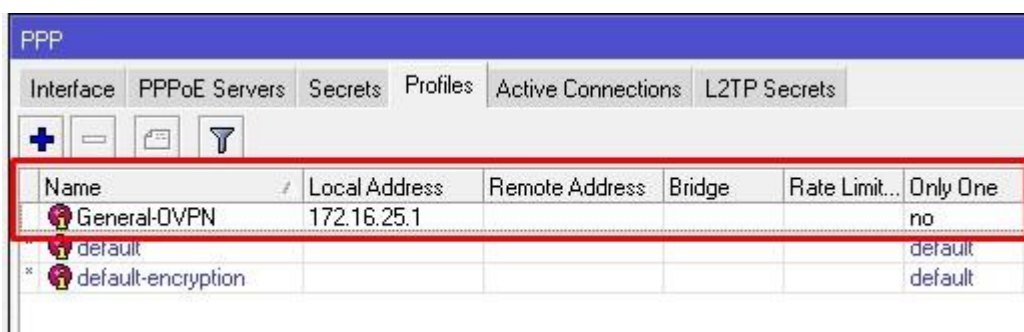
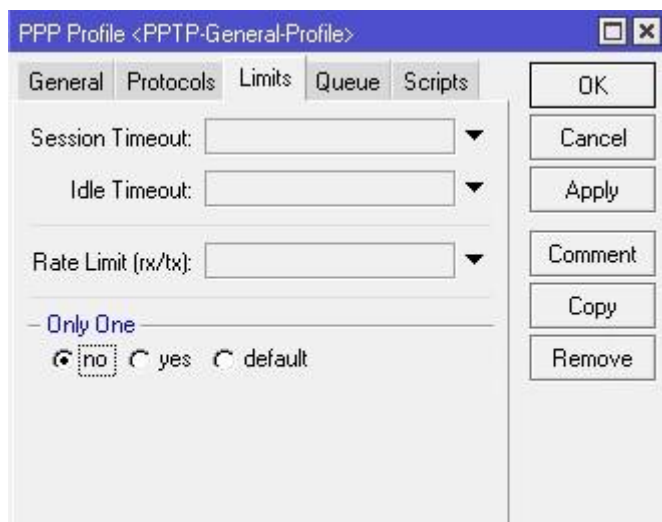
- no для Use MPLS;
- yes для Use Compression;
- yes для Use Encryption.

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

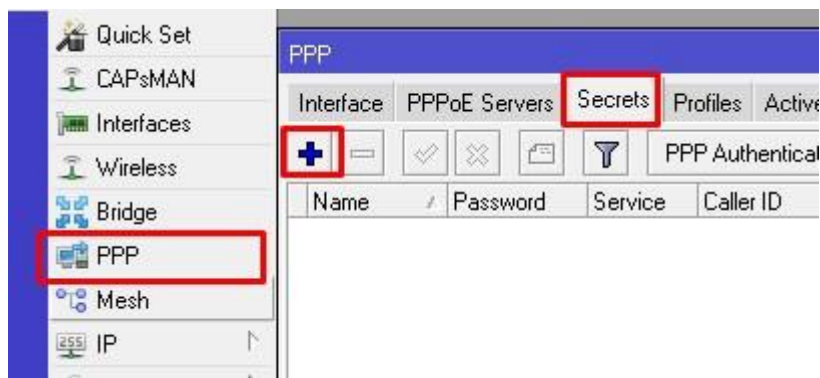
Теперь можно сохранять. Жмем Apply и OK. В списке должен появиться наш созданный профиль.

The screenshot shows the 'New PPP Profile' dialog box with the 'General' tab selected. The 'Name' field contains 'General-OVPN'. The 'Local Address' field contains '172.16.25.1'. The 'Change TCP MSS' section has 'yes' selected. The 'Use UPnP' section has 'no' selected. The 'Remote Address' field is empty. The 'Bridge' field is empty. The 'Bridge Port Priority' field is empty. The 'Bridge Path Cost' field is empty. The 'Bridge Horizon' field is empty. The 'Incoming Filter' field is empty. The 'Outgoing Filter' field is empty. The 'Address List' field is empty. The 'Interface List' field is empty. The 'DNS Server' field is empty. The 'WINS Server' field is empty. The 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove' buttons are on the right.

The screenshot shows the 'New PPP Profile' dialog box with the 'Limits' tab selected. The 'Use MPLS' section has 'no' selected. The 'Use Compression' section has 'yes' selected. The 'Use Encryption' section has 'yes' selected. The 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove' buttons are on the right.



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.

New PPP Secret

Name: OVPN-User-1

Password:

Service: ovpn

Caller ID:

Profile: General-OVPN

Local Address:

Remote Address: 172.16.25.2

Routes:

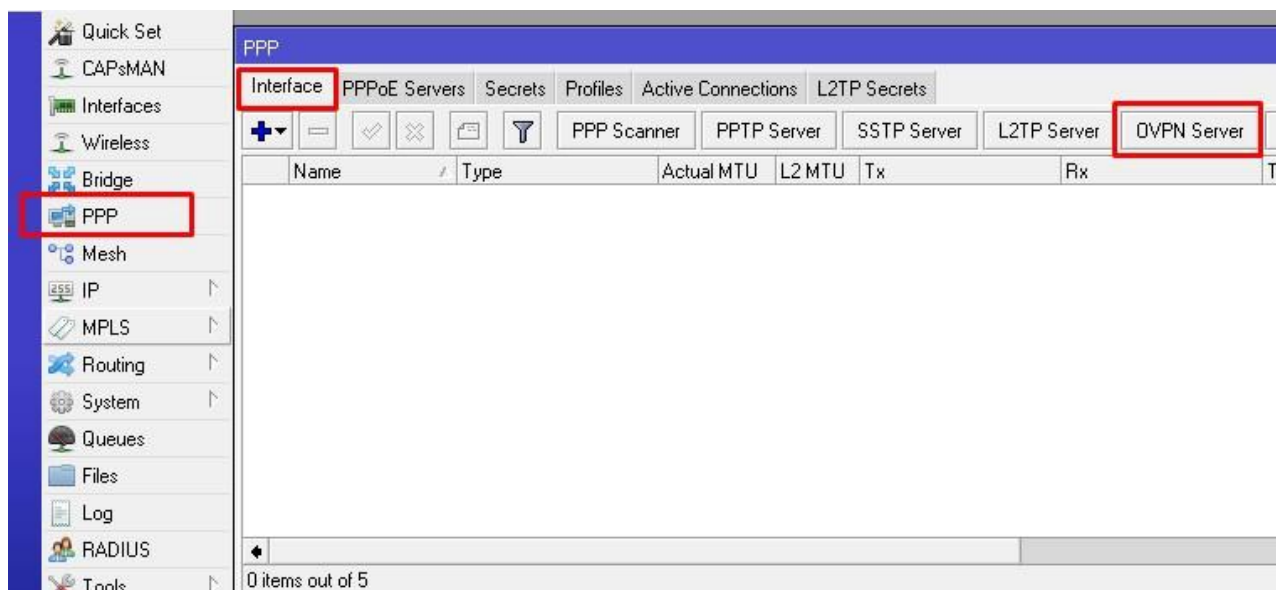
Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

OK Cancel Apply Disable Comment Copy Remove



- 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.

OpenVPN Server

☒ Enabled

Port: 1194

Mode: ip

Netmask: 24

MAC Address: FE:27:43:8D:A3:E1

Max MTU: 1500

Keepalive Timeout: 60

Default Profile: General-VPN

Certificate: ServerVPN

☐ Require Client Certificate

Auth.: ☒ sha1 ☒ md5 ☐ null

Cipher: ☒ blowfish 128 ☒ aes 128 ☐ aes 192 ☒ aes 256 ☐ null

OK Cancel Apply

Настройка Firewall

Далее нужно разрешить OpenVPN трафик на роутере.

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Mesh IP MPLS Routing System

Firewall

Filter Rules NAT Mangle Raw Service Ports

+ - [check] [X] [lock] [filter] [Reset Counters]

#	Action	Chain	Src. Address	Dst. Address
---	--------	-------	--------------	--------------

Добавляем правило.

Firewall Rule <172.16.10.2>1723>

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐ 172.16.10.2

Dst. Address:

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port: ☐ 1723

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☐ invalid ☐ established ☐ related ☒ new ☐ untracked

Connection NAT State:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Action – accept.

New Firewall Rule

General Advanced Extra Action Statistics

Action:

☐ Log

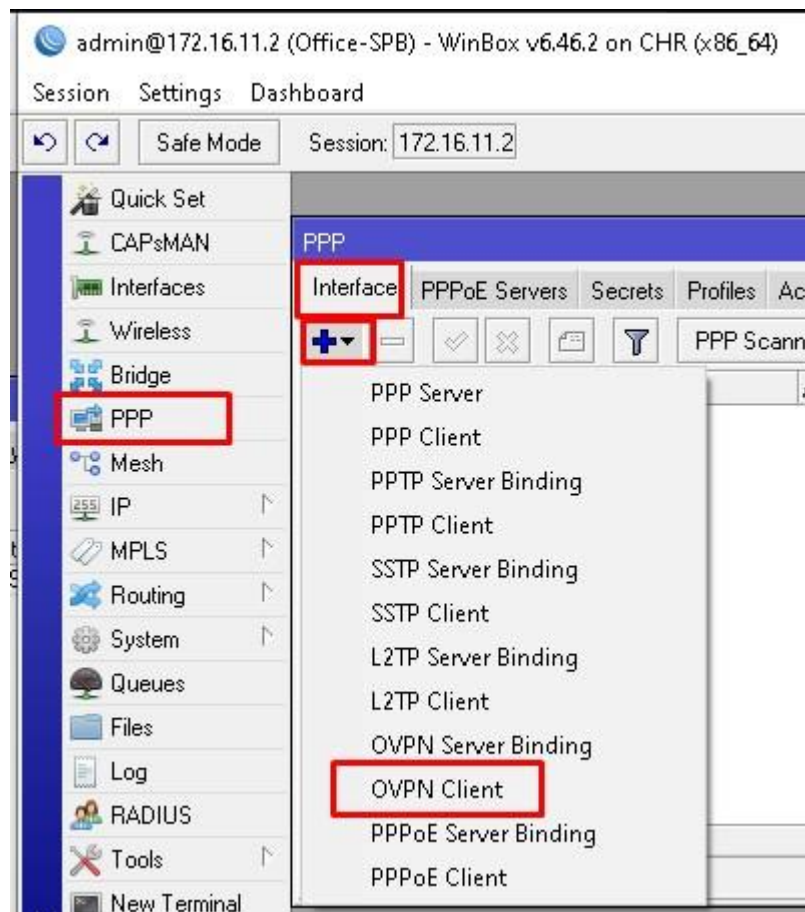
Log Prefix:

OK
Cancel
Apply
Disable
Comment
Copy
Remove

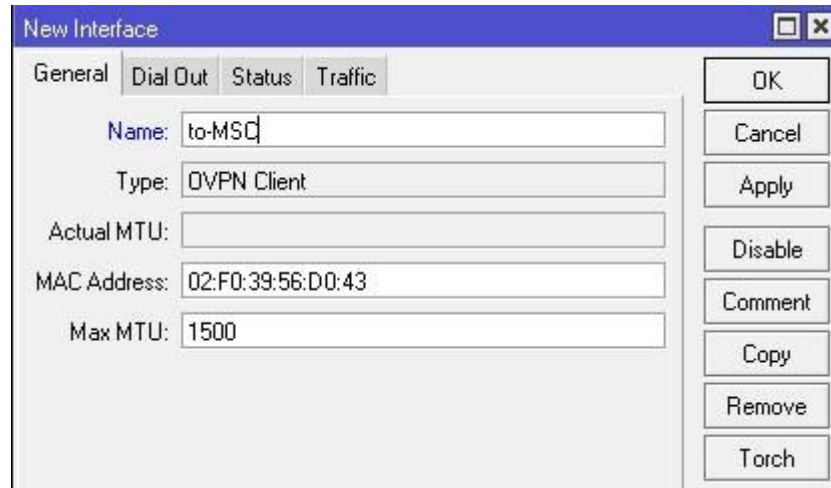
Сохраняем и переходим к клиентской части.

Конфигурирование клиента

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



Задаем имя интерфейса.



Открываем Dial Out и заполняем обязательные параметры.

New Interface

General | Dial Out | Status | Traffic

Connect To: 172.16.10.2

Port: 1194

Mode: ip

User: OVPN-User-1

Password: 1234

Profile: default

Certificate: none

☐ Verify Server Certificate

Auth: sha1

Cipher: aes 256

☐ Add Default Route

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

Сохраняем и открываем вкладку Status.

Interface <to-MS>

General | Dial Out | Status | Traffic

Last Link Down Time: Jan/18/2020 22:05:37

Last Link Up Time: Jan/18/2020 22:07:30

Link Downs: 3

Uptime: 00:06:11

Encoding: AES-256-CBC/SHA1

MTU: 1500

Local Address:

Remote Address:

enabled | running | slave | Status: connected

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

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-MSK
[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] >
```

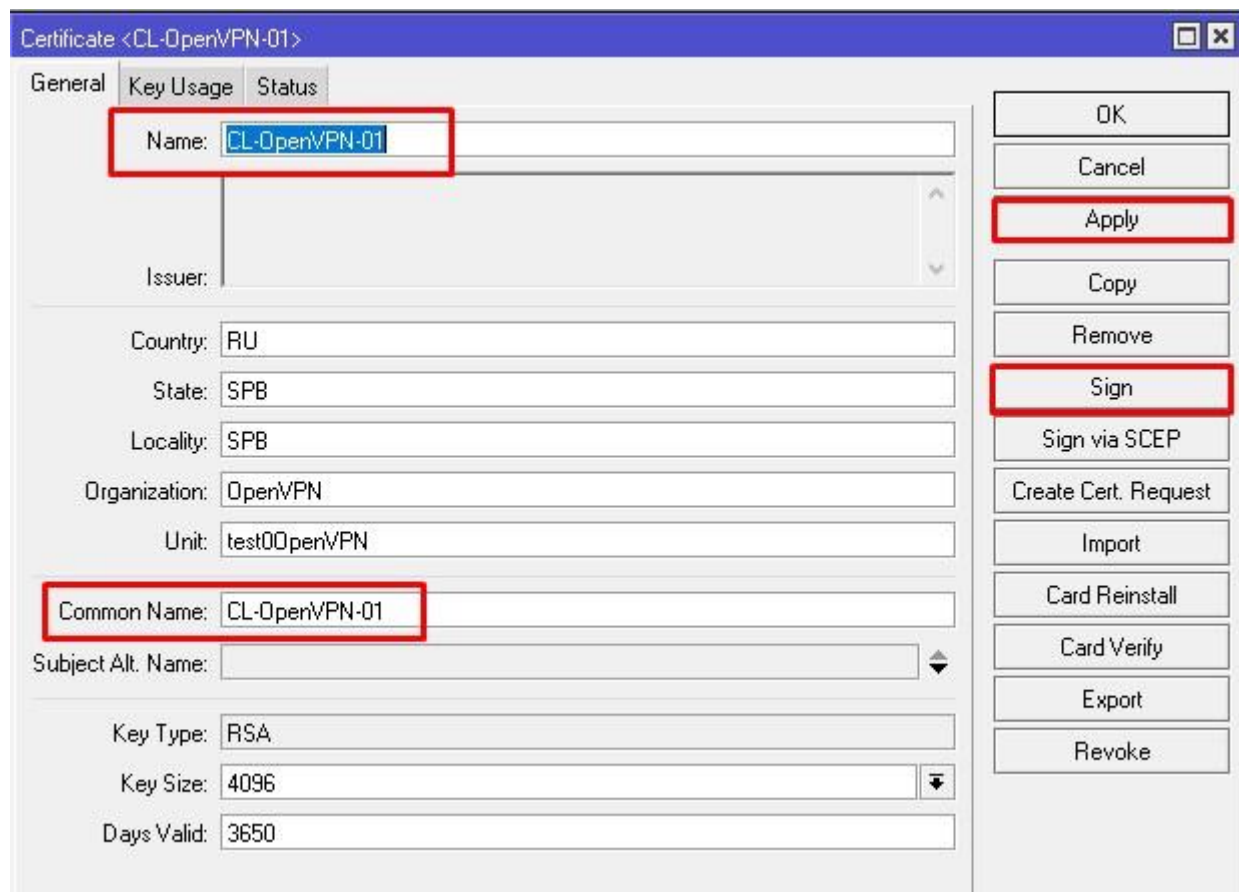
Ping-и идут, а значит с соединением все хорошо.

Настройка OpenVPN по сертификату

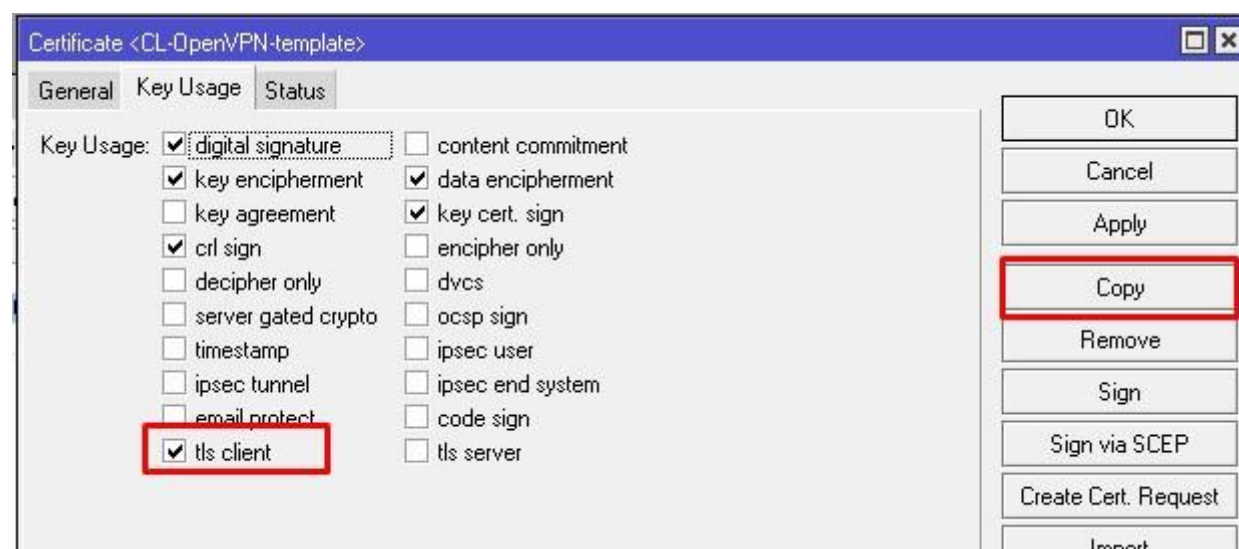
Здесь мы рассмотрим как настроить подключение по сертификату, выполним экспортирование и импортирование ключей для клиента и сервера.

Настройка сервера

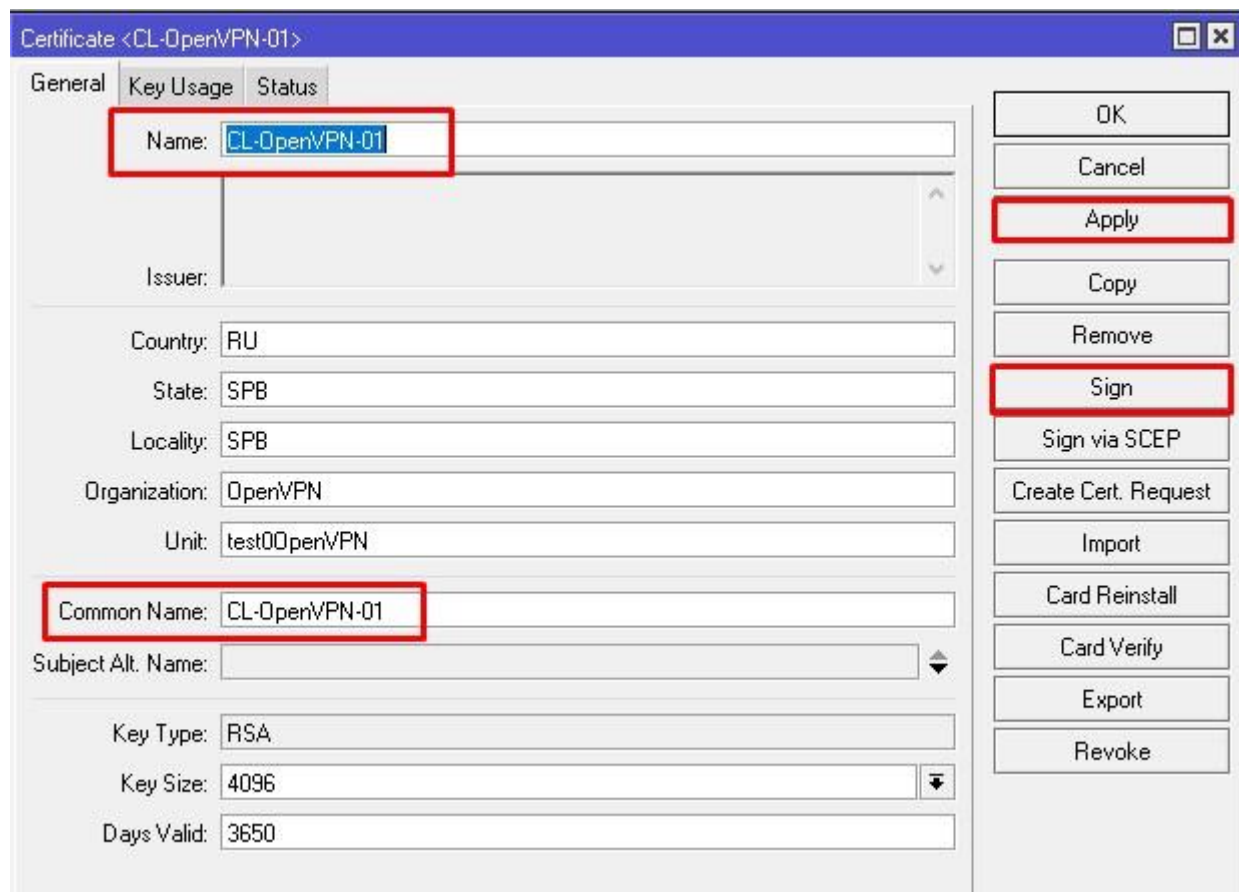
Ранее мы настроили аутентификацию по логину и паролю. Настроить аутентификацию только по клиентскому сертификату не получится в связи с ограничением операционной системы. Подключаемся на московский роутер, открываем Certificates и создаем новый шаблон.



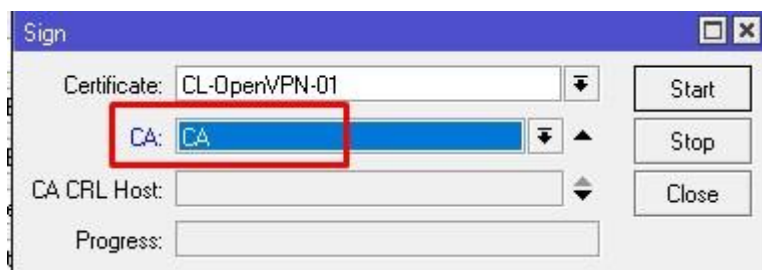
Key Usage. Обязательно ставим галочку на tls client.



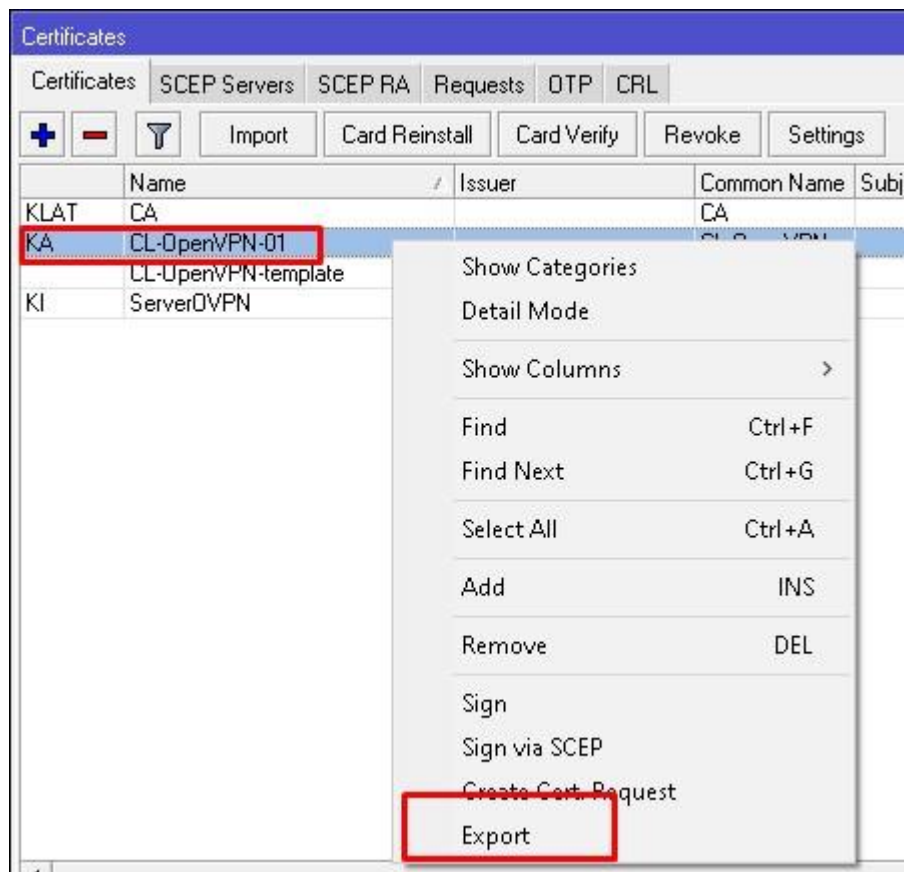
Сохраняем изменения и нажимаем Copy. Выбираем наш шаблон для пользователей и создаём копию. В Common Name уникальное имя. Далее нажимаем Apply и Sign.



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



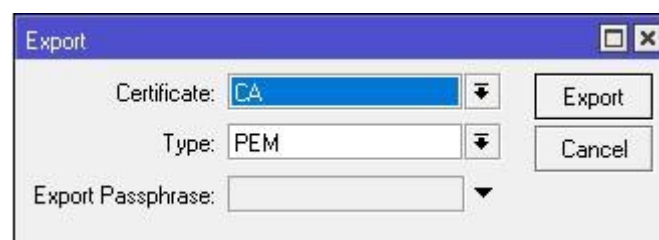
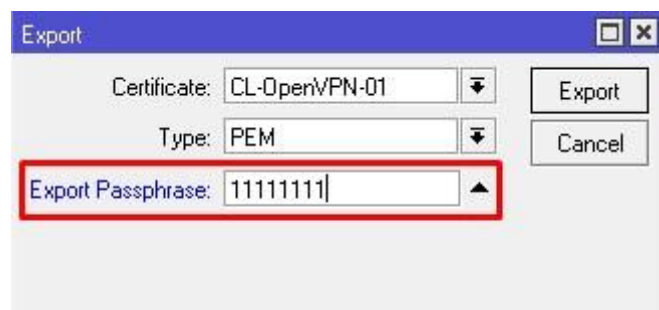
Далее нужно экспортировать и импортировать ключи на клиентский Mikrotik. Выбираем в списке и жмем Export.

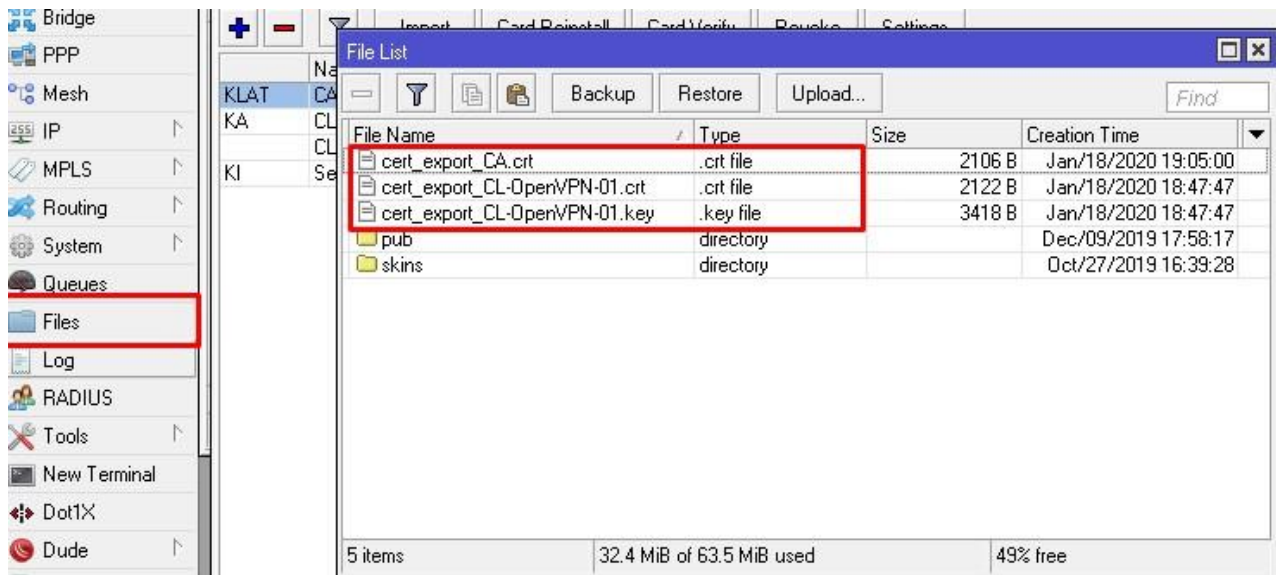


Для того чтобы выгрузить открытый и закрытый ключи, вбиваем пароль в поле Export Passphrase. Export.

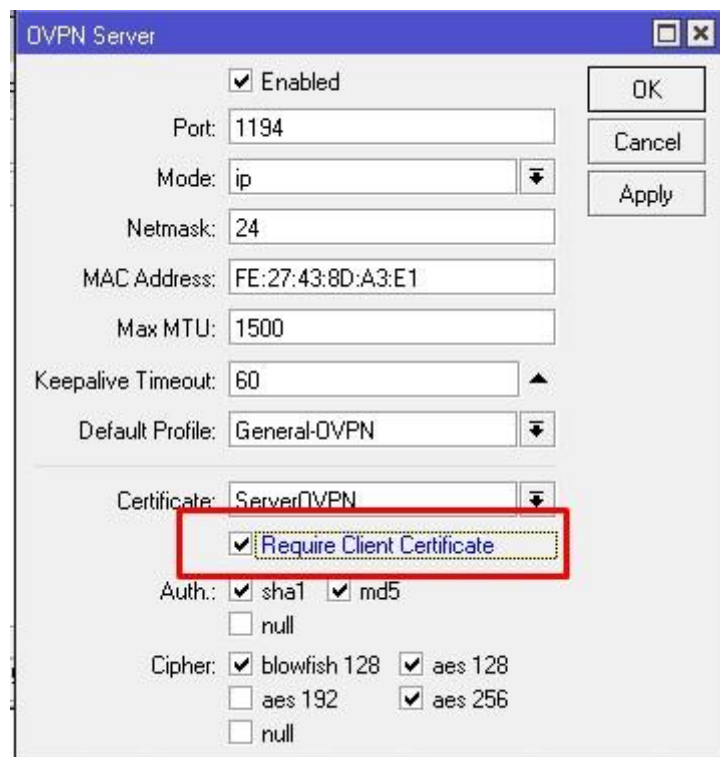
Далее нужно экспортировать открытую часть CA.

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



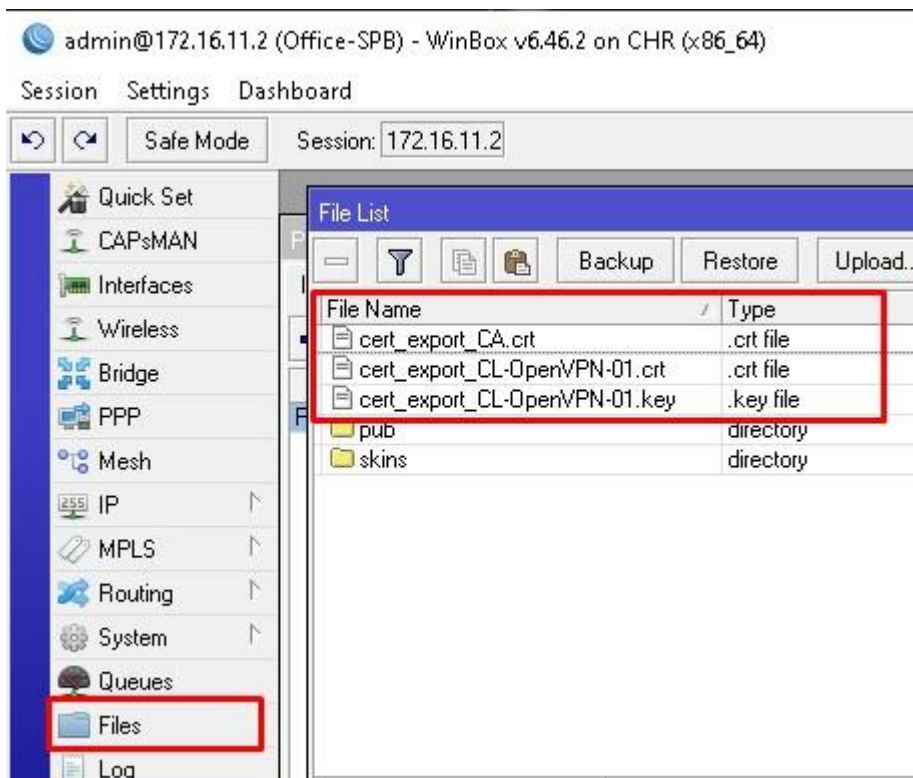


В настройках OVPN Server выставим чтобы проверялись клиентские сертификаты при подключении.



Настройка клиента

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



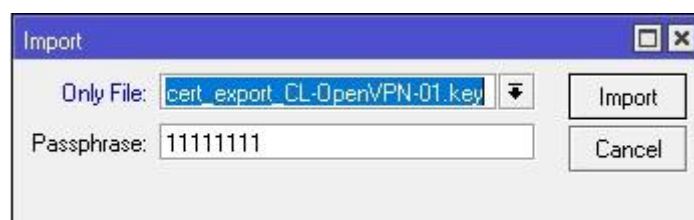
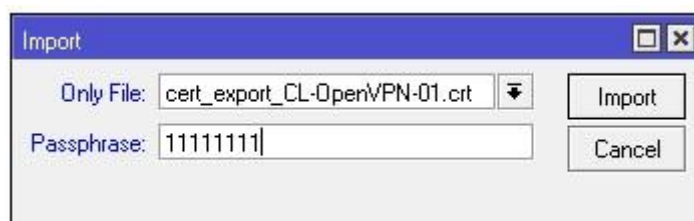
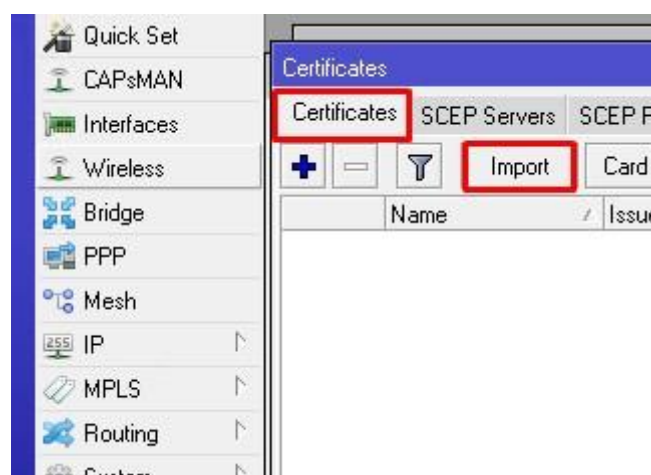
Переходим в Certificates и импортируем открытый и закрытый ключи.

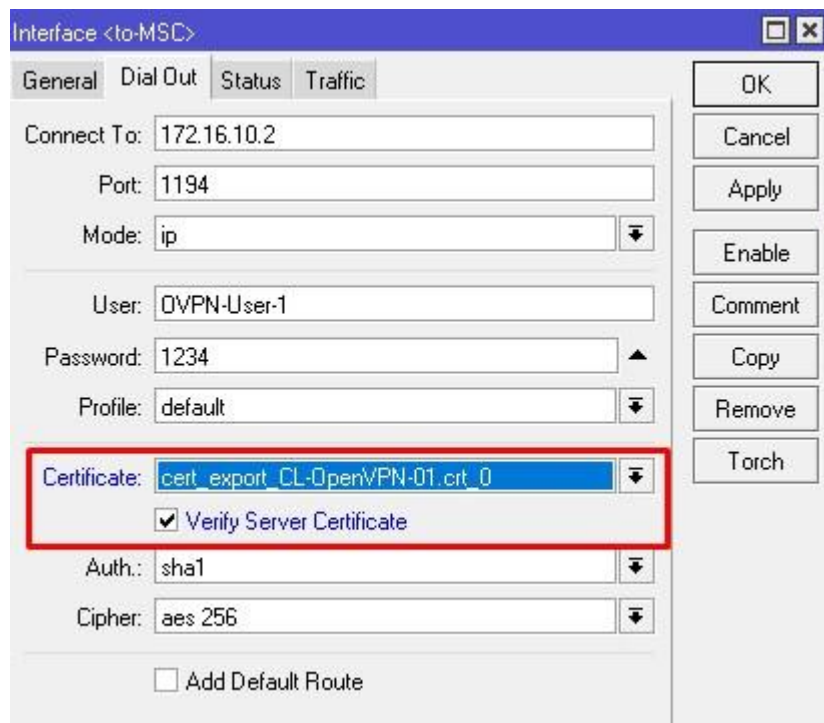
В выпадающем списке выбираем открытый ключ и вписываем пароль. Import.

Тоже самое с закрытым ключом.

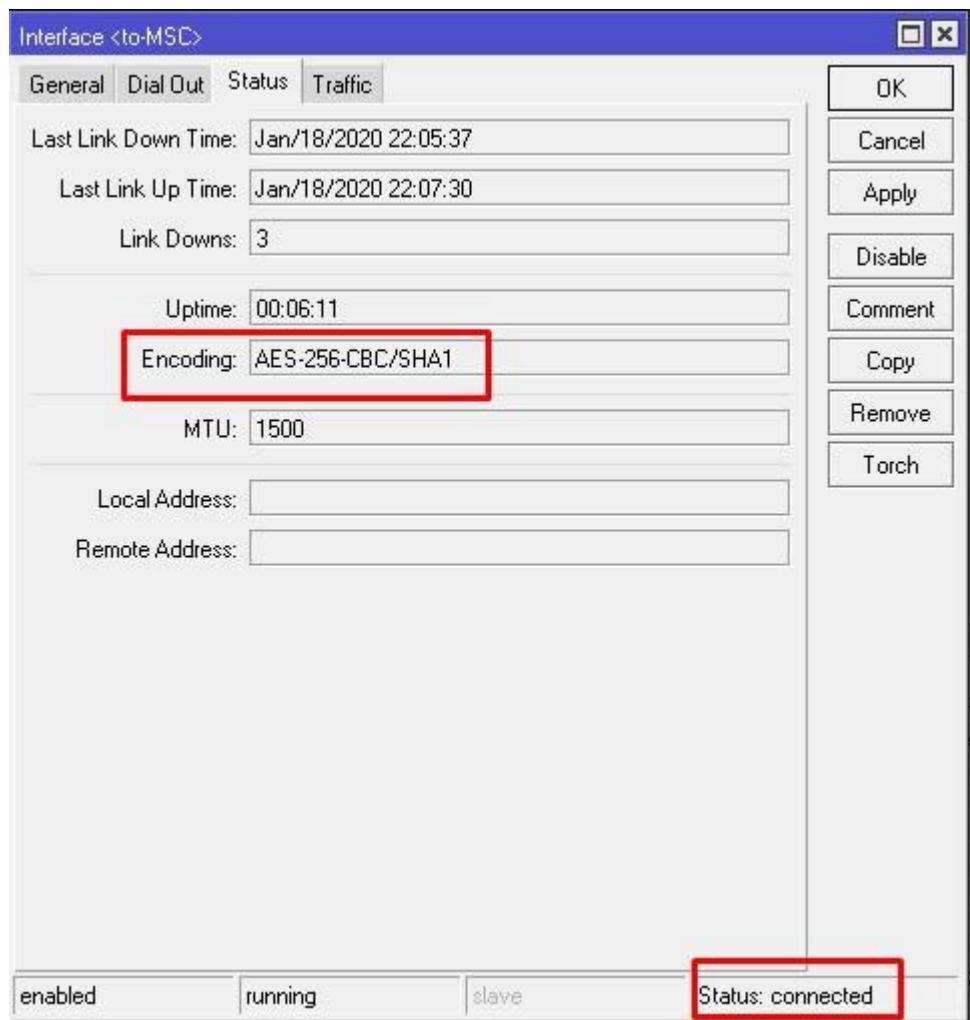
Далее импортируем CA.

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





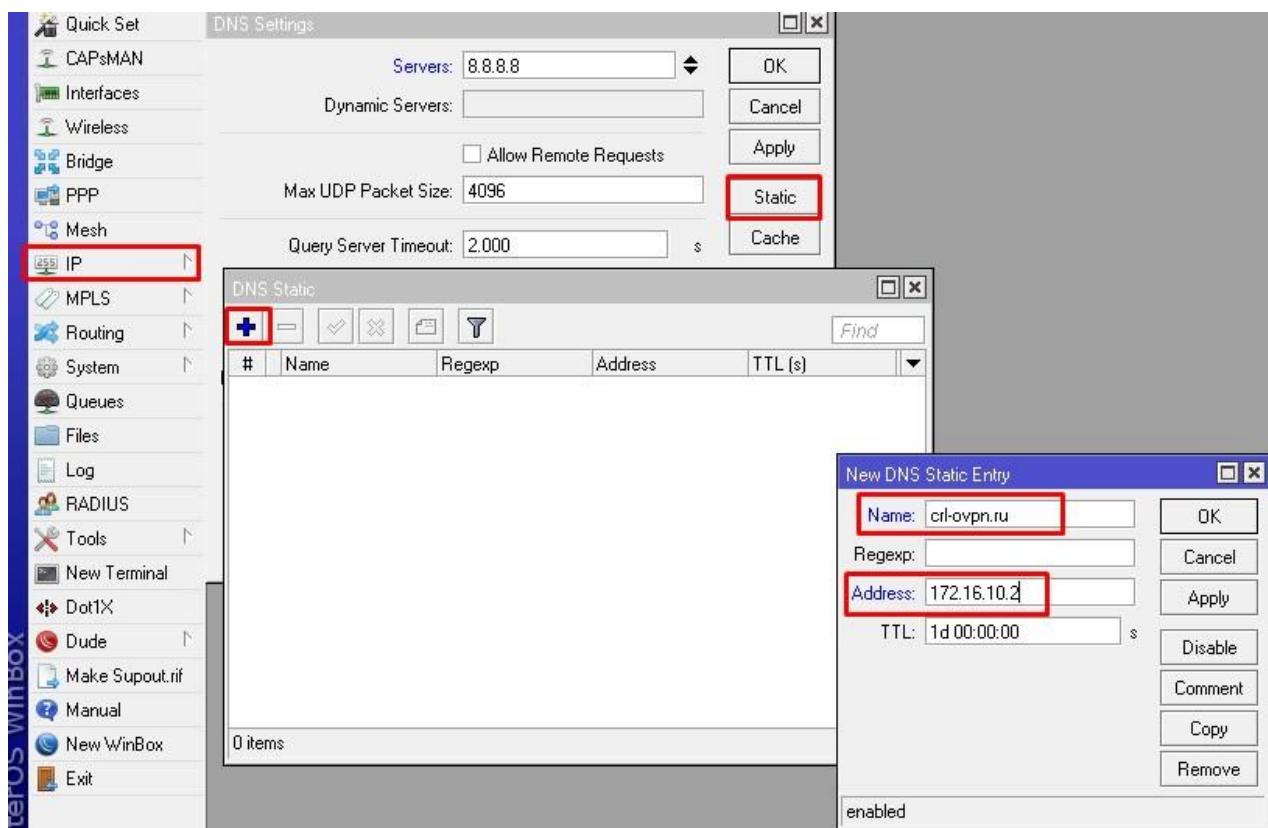
Соединение установилось.



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-MS
[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 srl-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](#).