

*MikroTik*

# OpenVPN-сервер на Mikrotik: от подключения мобильных устройств до десктопов

---



# Вопросы вебинара

---

- Общие сведения
- Настройка OpenVPN сервера без использования клиентских сертификатов
- Настройка с использованием клиентских сертификатов
- Конфигурация для подключения Windows к OpenVPN серверу
- Конфигурация для мобильных устройств
- Особенности правил Firewall
- Поиск проблем

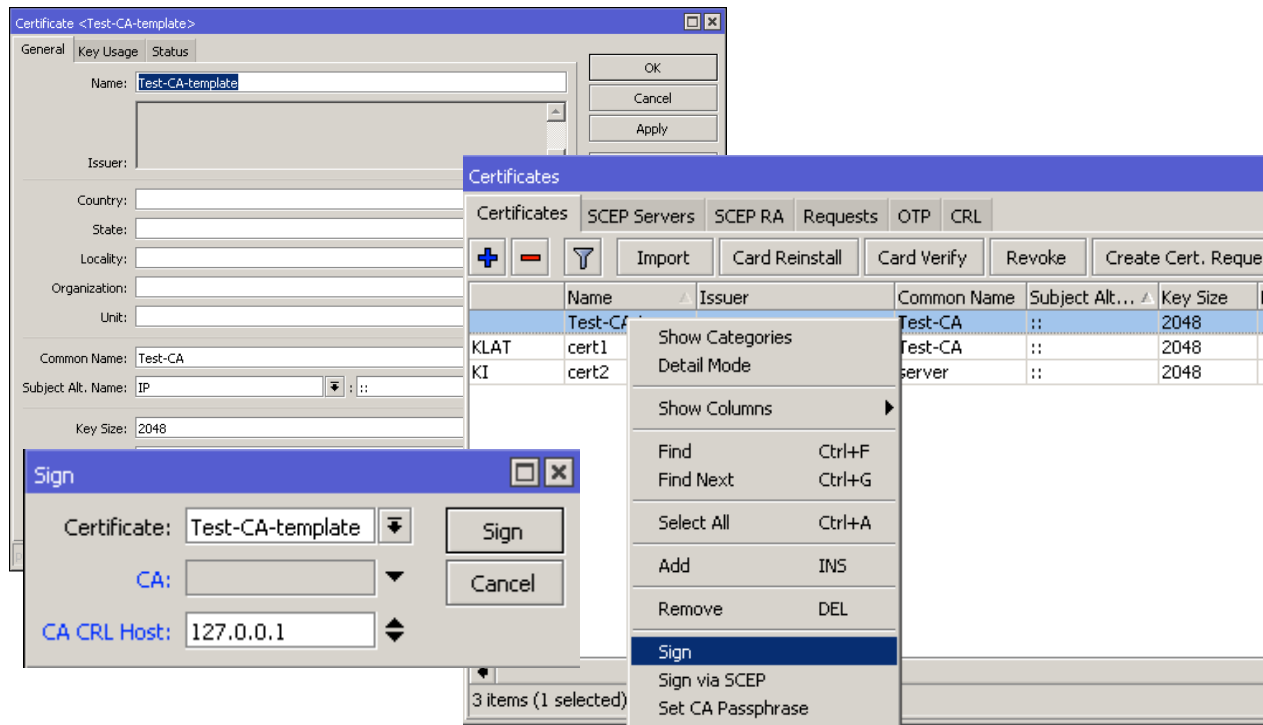


# OpenVPN

---

- **OpenVPN** – свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами.
- MikroTik RouterOS поддерживает как клиент так и сервер в режиме **TAP** и **TUN** по TCP протоколу
- Порт по умолчанию **TCP 1194**
- Для настройки требуется серверный сертификат

# OpenVPN создание CA сертификата



# OpenVPN создание сертификата сервера

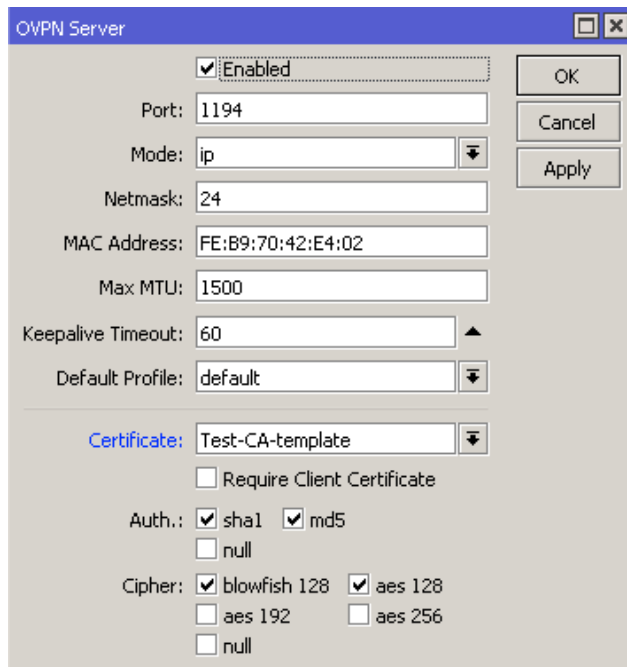
The screenshot shows the 'New Certificate' dialog in Mikrotik WinBox. The 'General' tab is active, and the 'Name' field is set to 'Template-server'. The 'Common Name' is 'server' and 'Subject Alt. Name' is 'IP'. The 'Key Size' is 2048 and 'Days Valid' is 3650. A context menu is open over the certificate list, with 'Sign' selected. A 'Sign' dialog box is also open, showing the 'Certificate' as 'Template-server' and the 'CA' as 'Test-CA-template'.

Name	Issuer	Common Name	Subject Alt...	Key Size
Template-ser...		server	::	2048
KLAT Test-CA		Test-CA	::	2048

Sign dialog fields:

- Certificate: Template-server
- CA: Test-CA-template
- CA CRL Host: [empty]

# OpenVPN настройка сервера



OVPN Server

Enabled

Port: 1194

Mode: ip

Netmask: 24

MAC Address: FE:B9:70:42:E4:02

Max MTU: 1500

Keepalive Timeout: 60

Default Profile: default

Certificate: Test-CA-template

Require Client Certificate

Auth.:  sha1  md5  
 null

Cipher:  blowfish 128  aes 128  
 aes 192  aes 256  
 null

OK  
Cancel  
Apply

# OpenVPN ethernet

- OpenVPN может работать в режиме ethernet.
- Интерфейс openvpn может быть добавлен в bridge

The screenshot displays three configuration panels in Mikrotik WinBox:

- OVPN Server:** Shows the server is enabled. Port is 1194, Mode is ethernet, Netmask is 24, MAC Address is FE:01:50:42:69:E4, Max MTU is 1500, Keepalive Timeout is 60, Default Profile is ovpn, and Certificate is gw-test1.integrasky.ru. Authentication is set to sha1 and md5, and Ciphers include blowfish 128, aes 128, aes 192, and aes 256.
- Interface <ovpn-out1>:** Shows the interface is connected to 100.64.100.1, Port is 1194, Mode is ethernet, User is ppp1, Password is ppp1, Profile is default, Certificate is none, Auth. is sha1, and Cipher is aes 256. There is an option to Add Default Route.
- Bridge:** Shows a table of bridge members:

Interface	Bridge
ether4	bridge2
ovpn-in1	bridge2

# Генерация сертификата CA и сервера

## Сертификат CA:

```
/certificate add name=template-CA country="" state="" locality="" organization="" unit="" common-name="test-CA" key-size=4096 days-valid=3650 key-usage=crl-sign,key-cert-sign
```

```
/certificate sign template-CA ca-crl-host=ip name="test-CA"
```

Примечание: ca-crl-host= – обязательный параметр, иначе список отзыва не будет создан; полный путь к списку отзыва будет указан в параметрах сертификата, графа "Точка распределения списка отзыва (CRL)"; в принципе, можно указать любой из ip-адресов нашего микротика, тот что укажем – и будет прописан в сертификате. Доменные имена параметром не поддерживаются, к сожалению.

## Сертификат сервера:

```
/certificate add name=template-SRV country="" state="" locality="" organization="" unit="" common-name="test-srv-OVPN" key-size=4096 days-valid=1095 key-usage=digital-signature,key-encipherment,tls-server
```

```
/certificate sign template-SRV ca="test-CA" name="test-srv-OVPN"
```

Примечание: в отличие от SSTP – OVPN не проверяет соответствие common-name сертификата сервера fqdn'у этого сервера



## Скрипты для генерации пользователей

---

```
/certificate add name=template-CL country="" state="" locality="" organization="" unit="" common-name="test-client-ovpn-template" key-size=4096 days-valid=3650 key-usage=tls-client
```

```
:local Vuser user24
```

```
:local password "Pass";
```

```
:local psk Pass123;
```

```
:local CA test-CA;
```

```
/certificate add name=$Vuser copy-from="template-CL" common-name=$Vuser
```

```
/certificate sign $Vuser ca="$CA" name="$Vuser"
```

```
/ppp secret add name=$Vuser password=$password profile=ovpn
```

```
/certificate export-certificate $Vuser export-passphrase=$psk
```

# Конфигурация для подключения Windows к OpenVPN серверу без сертификатов клиента

---

```
client
dev tap
proto tcp
remote IP 1194
float
auth-user-pass
verb 3
<ca>
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
</ca>
```

# Конфигурация для подключения Windows к OpenVPN серверу

client

dev tun #режим tun(ip) или tap(Ethernet)

proto tcp #протокол

remote ip-address port

resolv-retry infinite #если OpenVPN не удалось узнать имя удаленного хоста по DNS, то через указанное количество секунд попытаться переподключиться.

nobind #использовать динамический порт для подключения

persist-key # указывает не перечитывать файлы ключей при перезапуске туннеля.

persist-tun # оставляет без изменения устройства tun/tap при перезапуске OpenVPN.

auth-user-pass auth.cfg #указывается на клиентской стороне. Параметр не обязателен, если он отсутствует то будет предложено ввести пару логин/пароль. Файл должен содержать имя пользователя и пароль в двух строчках: username password

remote-cert-tls server #Для исключения возможности mitm атаки

verb 3 #устанавливает уровень информативности отладочных сообщений. Может принимать параметр от 0 до 11.

route 192.168.0.0 255.255.0.0 #маршруты

cert client.crt #клиентский сертификат - открытый

key client.key #клиентский закрытый ключ

ca CA.cr #сертификат CA

```
client
dev tun
proto tcp
remote ip-address port
resolv-retry infinite
nobind
persist-key
persist-tun
auth-user-pass
remote-cert-tls server
verb 3 route 192.168.0.0 255.255.0.0
<cert>
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
-----END RSA PRIVATE KEY-----
</key>
<ca>
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
</ca>
```

## Конфигурация для подключения мобильных устройств к OpenVPN серверу

---

```
openssl rsa -aes256 -in key.key -out key.key
```

## Особенности правил Firewall

---

- Для подключения к серверу используется один порт – указанный в настройках OpenVPN сервера
- Цепочка для правила – INPUT
- Для ограничения трафика от клиентов можно воспользоваться IN-interface – “all ppp”
- Так же можно использовать статические интерфейсы для создания правил – OVPN-Server binbing
- Через профиль можно добавить интерфейсы клиентов в определенный интерфейс лист
- Через профиль можно добавить ip адреса клиентов в определенный адрес лист

# Поиск проблем

---

- **Включение логирования на MikroTik**
  - `/system logging action`
  - `add name=openvpn target=memory`
  - `/system logging`
  - `add action=openvpn topics=ovpn,debug`
- **Включение логирования на клиентской стороне**
  - `verb 3` #устанавливает уровень информативности отладочных сообщений. Может принимать параметр от 0 до 11.

# СПАСИБО ЗА ВНИМАНИЕ

Приходите на наши курсы по  
Mikrotik и Asterisk

*Mikro***Tik**

