

Mikrotik: сервер OpenVPN и Ubuntu в качестве клиента

Курс «Настройка оборудования MikroTik»

Освоить MikroTik вы можете с помощью онлайн-курса «Настройка оборудования MikroTik». В курсе изучаются все темы из официальной программы МТСНА. Автор – официальный тренер MikroTik. Материал подходит и тем, кто уже давно работает с оборудованием MikroTik, и тем, кто еще не держал его в руках. В состав входят 162 видеоурока, 45 лабораторных работ, вопросы для самопроверки и конспект. [Узнать подробности](#)

Задача:

- Mikrotik в качестве сервера OpenVPN, Ubuntu в качестве клиента
- Генерация сертификатов на Mikrotik

Настраиваем Mikrotik

Создаем сертификаты

Создаем сертификаты: CA, сервера OpenVPN, клиента OpenVPN как описано тут: [Mikrotik: работа с сертификатами](#)

Экспортируем сертификаты: ca.crt, client1.crt, client1.key (с паролем)

Создаем профиль

Открываем PPP / Profiles, создаем новый (не все из указанных опций нужны, смотрите сами):

- Закладка General
 - Name: openvpn-profile
 - Local Address: 10.10.10.1
 - Change TCP MSS: Yes
- Закладка Protocols
 - Use Compression: Yes
 - Use Encryption: Yes
- Закладка Limits
 - Only One: No

Создаем пользователя

Открываем PPP / Secrets, создаем нового пользователя:

- Name: ovpn-client1
- Password: \$ecretP@\$word
- Service: ovpn
- Profile: openvpn-profile
- Remote-Address: 10.10.10.2 (или можно сделать через пул адресов)

Включаем OpenVPN

Открываем PPP / OVPN Server, включаем:

- Enabled: включаем
- Port: 1194
- Mode: ip
- Default-profile: openvpn-profile
- Certificate: Выбираем сертификат сервера (не CA!)
- Require Client Certificate: включаем для проверки сертификата клиента
- Auth: sha1, остальное отключаем
- Cipher: aes 256, остальное отключаем

Создаем интерфейс для клиента

Это необязательно, но так удобнее работать для разрешения трафика.

Открываем PPP / Interface и создаем OVPN Server Binding

- Name: OVPN-Client1
- User: ovpn-client1

Разрешаем трафик

Открываем порт OpenVPN чтобы клиенты могли подключаться.

Не забываем поднять правила вверх списка чтобы они не попадали под запреты!

Открываем IP / Firewall, создаем новое правило:

- Chain: input
- Protocol: 6 (tcp)
- Dst. Port: 1194
- Action: Accept

При необходимости можете ограничить интерфейс и адреса с которых будет идти подключение.

Разрешаем трафик через VPN, открываем IP / Firewall, создаем 3 новых правила (зачем именно так - отдельный вопрос):

- Правило input
 - Chain: input
 - In. Interface: OVPN-Client1
 - Action: accept
- Правило forward
 - Chain: forward
 - In. Interface: OVPN-Client1
 - Action: accept
- Правило output
 - Chain: output
 - Out. Interface: OVPN-Client1
 - Action: accept

Настраиваем Ubuntu

Устанавливаем OpenVPN на Ubuntu

Подробно описано тут: [Установка OpenVPN в Ubuntu](#)

Настраиваем OpenVPN как клиент на Ubuntu

Копируем сертификаты ca.crt, client1.crt, client1.key (с паролем) на сервер в папку /etc/openvpn

Снимаем пароль с client1.key (иначе при запуске OpenVPN будет его требовать, а нам нужно чтобы все работало автоматически):

```
openssl rsa -in client1.key -out client1.key
```

Создаем конфигурационный файл /etc/openvpn/client.conf

XXX.XXX.XXX.XXX - адрес Mikrotik

```
client
dev tun
proto tcp
remote XXX.XXX.XXX.XXX 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client1.crt
key client1.key
remote-cert-eku 'TLS Web Server Authentication'
cipher AES-256-CBC
auth SHA1
auth-nocache
```

```
auth-user-pass client1.txt
user nobody
group nogroup
route 10.10.10.0 255.255.255.0 10.10.10.1
verb 3
mute 20
```

Создаем файл /etc/openvpn/client1.txt с логином и паролем:

```
ovpn-client1
Password: $ecretP@$word
```

Убираем права на файлы для всех пользователей кроме root:

```
chown root:root ca.crt client1.crt client1.key client1.txt client.conf
chmod 600 ca.crt client1.crt client1.key client1.txt client.conf
```

Запускаем клиента, смотрим логи, проверяем работу:

```
systemctl start openvpn@client
```

Включаем автоматический запуск OpenVPN при старте сервера:

```
systemctl enable openvpn@client
```

From:
<https://wiki.rtzra.ru/> - RTzRa's hive

Permanent link:
<https://wiki.rtzra.ru/software/mikrotik/mikrotik-ovpn-ubuntu>

Last update: **2020/11/08 21:34**

