

## Настройка подключения OpenVPN.

Для подключения абонентов по протоколу OpenVPN, необходимо следующее:

- Создать корневой и конечный сертификаты в модуле Сертификаты. При создании конечного сертификата на вкладке «Использование ключа» в поле «Шаблон» следует выбрать значение «VPN-сервер».

### Данные сертификата VPN-корневой

---

**Общее**

Название: VPN-корневой  
Код страны: RU - Russian Federation  
Имя или адрес хоста: test.ru

**Настройки**

Тип сертификата: CA  
Алгоритм: SHA 256  
Тип шифрования: RSA  
Создан: 06.11.2019  
Действует до: 07.11.2020  
Длина ключа: 2048 бит

**Использование ключа**

Использование ключа: Certificate Sign  
CRL Sign

### Данные сертификата Openvpn-сервер

**Общее**

Название: Openvpn-сервер  
Код страны: RU - Russian Federation  
Имя или адрес хоста: test.ru

**Настройки**

Тип сертификата: Конечный сертификат  
Алгоритм: SHA 256  
Тип шифрования: RSA  
Создан: 06.11.2019  
Действует до: 07.11.2020  
Длина ключа: 2048 бит

**Использование ключа**

Использование ключа: Digital Signature  
Key Encipherment  
Расширенное использование ключа: TLS Web Server Authentication  
Netscape расширение: SSL Server

**Ок** **Отмена**

- Добавить OpenVPN-сеть в модуле Провайдеры и сети. Для того, чтобы пользователи могли подключаться к ресурсам локальных сетей ИКС, необходимо установить флаг «Передать клиенту маршрут по умолчанию» и выбрать из списка сети, которые нужно маршрутизировать.

## Добавление OpenVPN-сети

Основные настройки    Шифрование и сертификаты

Название \*    Ip-адрес/Префикс \*

Супер VPN    10.8.0.0/24

Протокол    Порт сервера \*

UDP    1194

Использовать NAT

Разрешить трафик между клиентами

Передать клиенту маршрут по умолчанию

Передать клиентам маршруты до сетей

Мульти-локалка (192.168.17.242/24) ✕

Передать клиентам DNS сервера

Передать клиентам DNS сервера

Разрешить управление ИКК через веб

Разрешить управление ИКК через SSH

Добавить    Отмена

- В качестве сертификатов указать предварительно сгенерированные сертификаты из п.1.

### Добавление OpenVPN-сети

Основные настройки      Шифрование и сертификаты

Алгоритм шифрования: AES-256-CBC      Алгоритм хеширования: SHA256

Включить сжатие LZO

link-MTU \*: 1500

Корневой сертификат \*: VPN-корневой ✕      Сертификат сервера \*: Openvpn-сервер ✕

**Добавить**      Отмена

- Перейти в модуль VPN - Пользователи и отметить флажками пользователей, которым будет разрешено подключаться по протоколу OpenVPN, при этом будет предложено выбрать к какой из созданных сетей (если их несколько) будет подключаться пользователь. Важно: необходимо нажать кнопку «Сохранить», чтобы изменения вступили в силу.

Муми-дол > VPN-сервер > Пользователи      Туге Янссон      19

VPN-сервер    Настройки    **Пользователи**    Текущие сеансы    События    Журнал

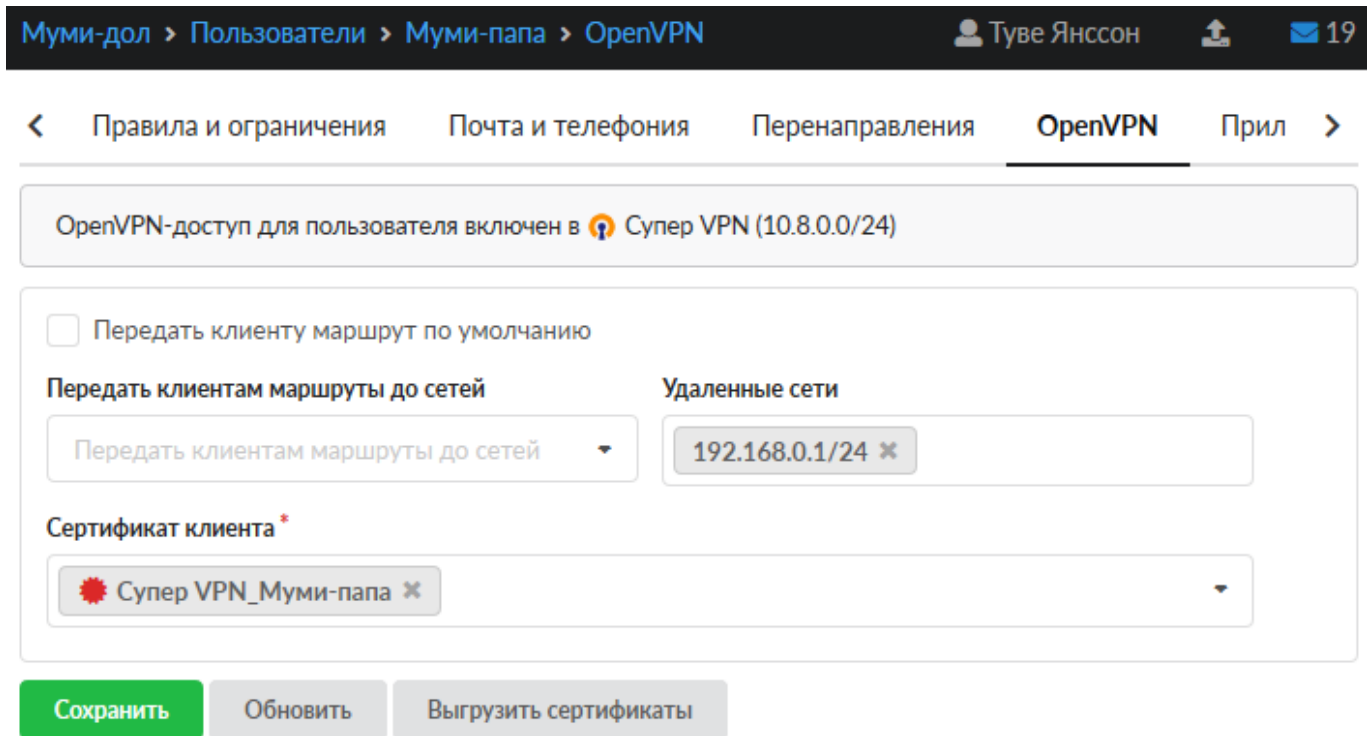
Добавить    Удалить    Выключить    Редактировать

Имя	Логин	Ip-адреса из Vpn-сетей	Vpn-доступ	OpenVPN-доступ
Корневая группа			<input type="checkbox"/>	<input type="checkbox"/>
Муми-дол			<input type="checkbox"/>	<input type="checkbox"/>
Мумики			<input type="checkbox"/>	<input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24)
Муми-мама	mumi3		<input type="checkbox"/>	<input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24)
Муми-папа	mumi2		<input type="checkbox"/>	<input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24)
Муми-троль (месячная квота исчерпана)	mumi1		<input type="checkbox"/>	<input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24)
Снорки			<input type="checkbox"/>	<input type="checkbox"/>

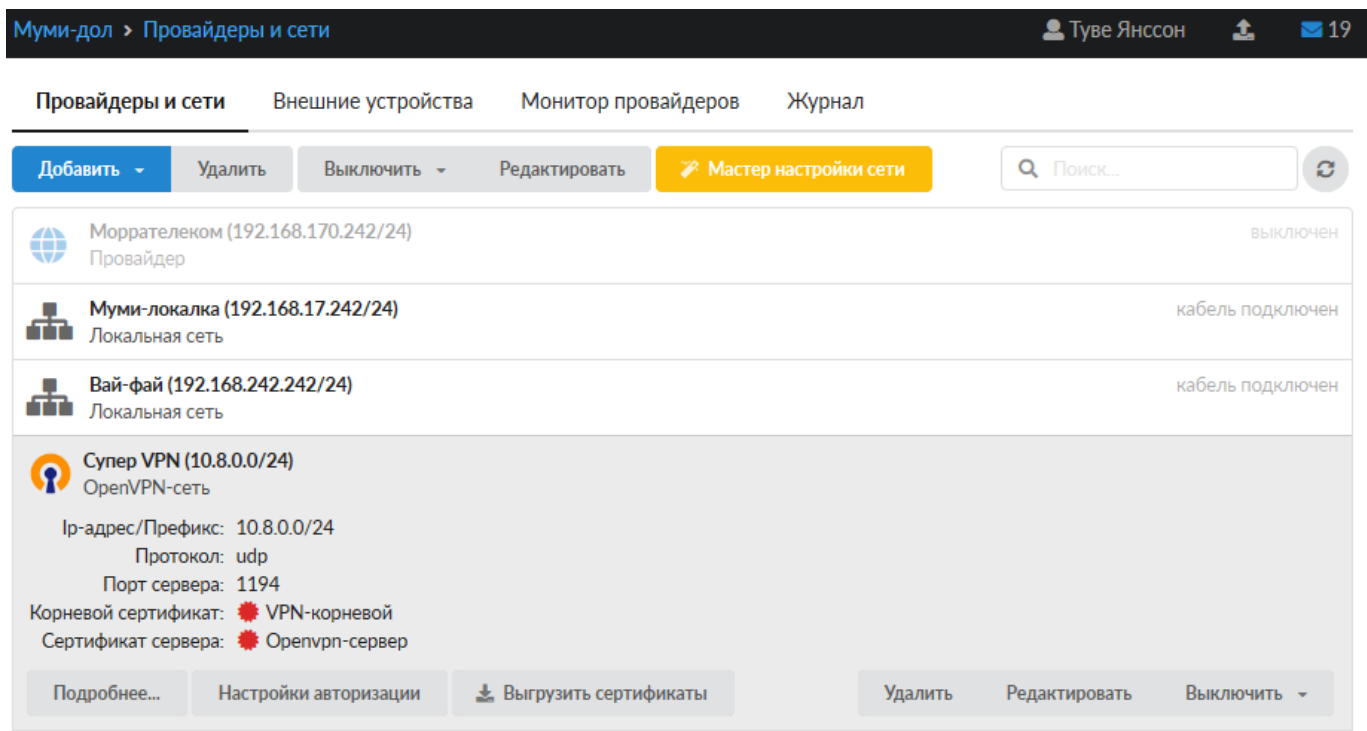
**Сохранить**    Обновить

- Перейти в индивидуальный модуль пользователя, вкладка OpenVPN. Если необходимо настроить маршрутизацию из локальной сети ИКС до других ресурсов в локальной сети

пользователя, то необходимо прописать сеть, в которой находится данный пользователь.



- В модуле Провайдеры и сети необходимо выгрузить клиентские сертификаты для подключения пользователей



- Для подключения пользователя, ему необходимо установить на своем компьютере утилиту OpenVPN (<https://openvpn.net/>), после чего распаковать содержимое папки с именем пользователя из архива выгруженных сертификатов в папку <путь до установки>\config, запустить утилиту и выполнить подключение.

# Прекращение доступа Пользователя к OpenVPN

Для того чтобы отозвать у Пользователя доступ к OpenVPN, необходимо перейти в Меню - Сеть - VPN - вкладка «Пользователи», напротив необходимого Пользователя снять флаг «OpenVPN-доступ» и нажать «Сохранить». При этом доступ у Пользователя прекратится сразу, даже если у него было активное соединение. В Меню - Защита - Сертификаты, созданный ранее автоматический сертификат Пользователя, будет серым с состоянием «сертификат отозван». **ВНИМАНИЕ:** отозванный сертификат не рекомендуется удалять из модуля «Сертификаты», иначе этот сертификат пропадёт из списка отозванных и Пользователь с таким сертификатом вновь получит доступ к OpenVPN. При удалении Пользователя из «ИКС», который имеет доступ к OpenVPN, его сертификат будет отозван.

CA	не зашифрован	34.04.2020	15.04.2021	test.ru		
ServerVPN	Ключевый сертификат	не зашифрован	34.04.2020	15.04.2021	test.ru	
Новый OpenVPN ccm, OpenVPN	Ключевый сертификат	не зашифрован	34.04.2020	14.04.2021	test	сертификат отозван
Новый OpenVPN ccm, OpenVPN	Ключевый сертификат	не зашифрован	34.04.2020	15.04.2021	test	

From: <https://doc-old.a-real.ru/> - Документация

Permanent link: [https://doc-old.a-real.ru/doku.php?id=ics70:openvpn\\_setup&rev=1586874088](https://doc-old.a-real.ru/doku.php?id=ics70:openvpn_setup&rev=1586874088)

Last update: 2020/04/14 17:21

