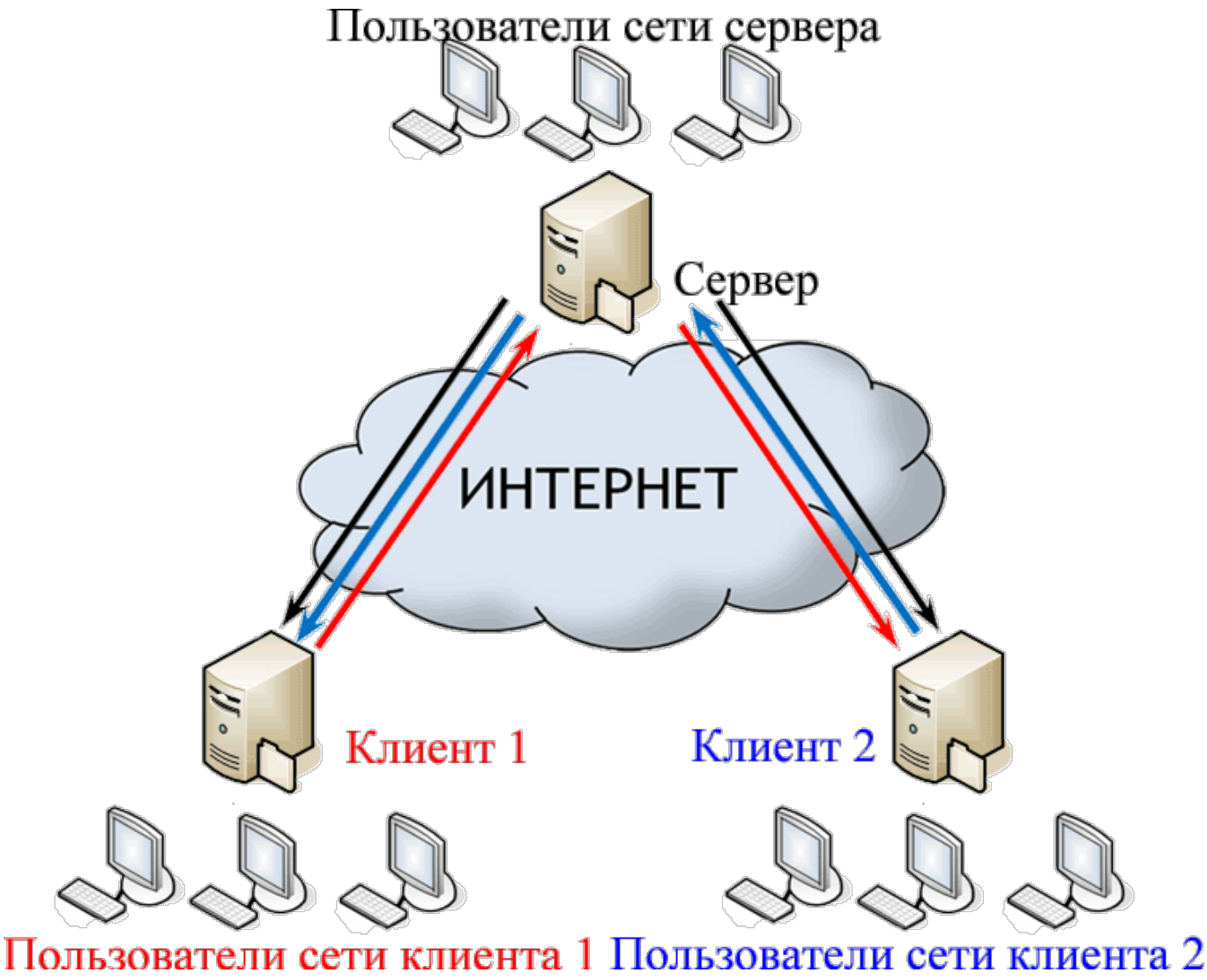
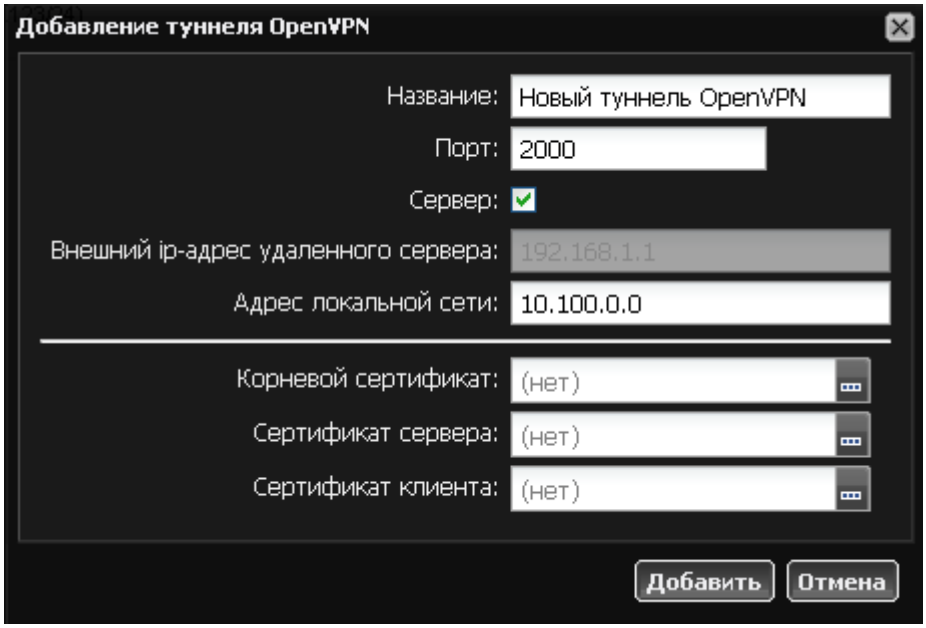
Туннель OpenVPN

OpenVPN — свободная реализация технологии VPN с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за NAT-firewall, без необходимости изменения их настроек.





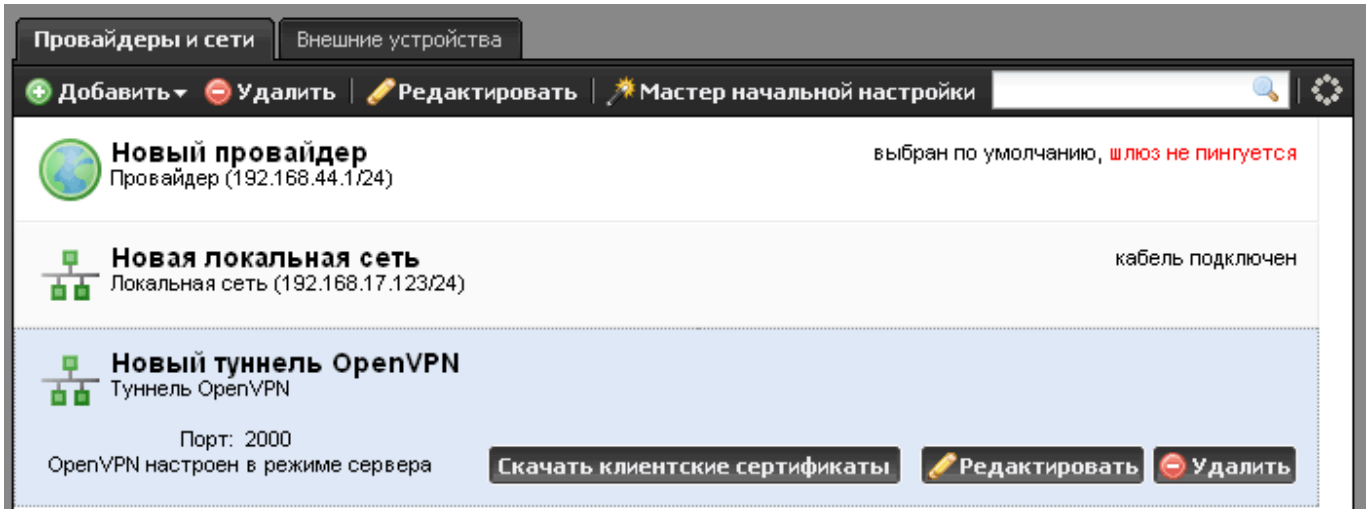
Система туннелей OpenVPN построена таким образом, что одна из машин выбирается сервером, а все остальные - клиентами. На сервере прописывается адресация пространства внутри openVPN-сети (рекомендуется оставить значение по умолчанию) и размещаются SSL-сертификаты, а на клиентах указывается внешний ip-адрес сервера. Также, указывается порт обмена данными, что позволяет подключаться к серверу, который находится за межсетевым экраном или NAT, при помощи перенаправления портов.

Для настройки OpenVPN-туннеля между двумя ИКС необходимо выполнить следующие действия:

1. Добавить новый туннель OpenVPN
2. Указать адресацию внутренней сети для маршрутизации между клиентами
3. Создать и добавить сертификаты защищенного соединения
4. Добавить в межсетевой экран необходимые разрешающие правила.

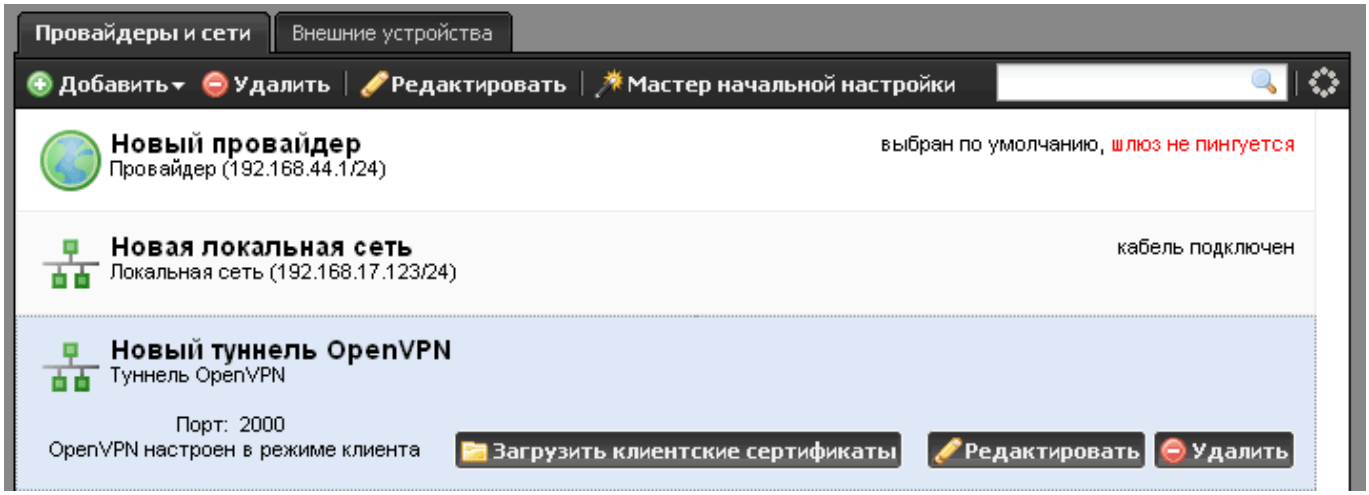
После чего все действия необходимо произвести на всех клиентах с указанием режима работы “клиент”.

Чтобы прописать необходимые сертификаты от сервера клиентам, сделайте следующее:



1. На сервере выделите созданный OpenVPN-туннель и нажмите кнопку «Скачать клиентские

сертификаты». Сохраните полученный архив.



2. На каждом из клиентов выделите созданный OpenVPN-туннель и нажмите кнопку «Загрузить клиентские сертификаты». Укажите ресурс, где хранится скачанный архив и загрузите его.