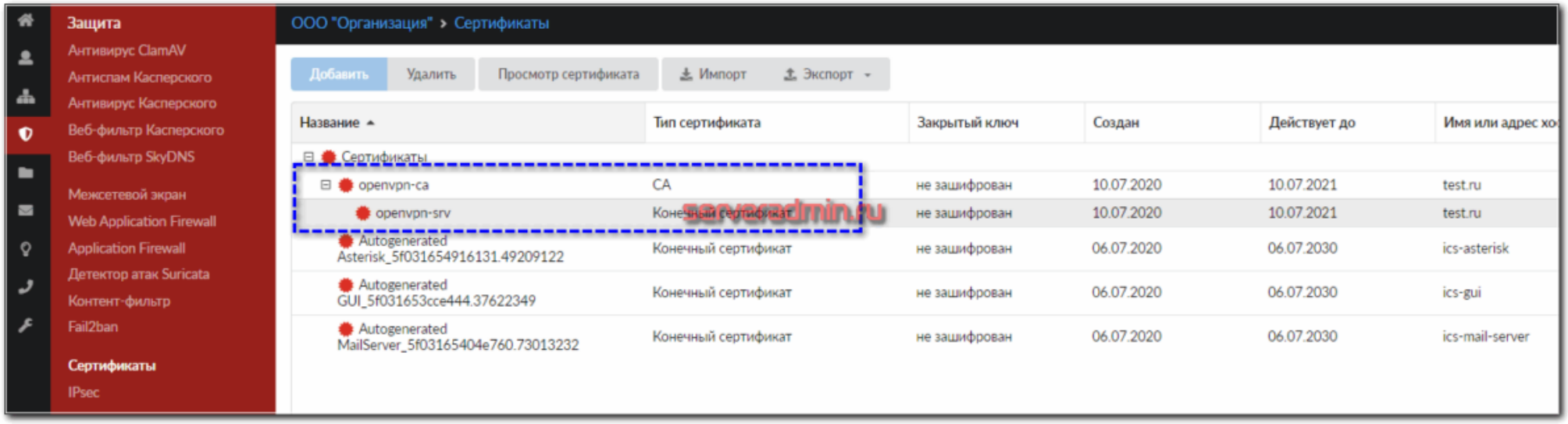


Некоторое время назад я писал заказной обзор на интернет шлюз ИКС от отечественных разработчиков. 22 июня 2020 года у них вышел новый релиз. У меня заказали его анонс и разбор. Для того, чтобы не повторяться с прошлым материалом, я постараюсь интересно и полезно дополнительно рассказать о том, что можно настроить с помощью этого шлюза.

Содержание

Введение

Подробно о том, что такое интернет шлюз ИКС я рассказал в предыдущей статье. Сейчас не хочется повторяться и еще раз разбирать тему, поэтому

коротко по пунктам перечислю его основной функционал. В общем и целом это программный шлюз на базе ОС Freebsd, с помощью которого можно:

1. Настроить прокси сервер с разбором всего трафика в том числе с помощью MITM для расшифровки https соединений.
2. Сделать ограничения доступа к сайтам на основе готовых списков от Минюста, Госнаркоконтроля и т.д.
3. Использовать списки пользователей и групп для централизованного ограничения и управления доступом и отчетами.
4. Настроить свои VPN туннели или подключиться к существующим на базе стороннего оборудования.
5. Запустить базовый функционал следующих сервисов - почта, файловый сервер, ip телефония, jabber.

При всем при этом интернет шлюз ИКС умеет:

- Настраиваться полностью через web интерфейс. В консоль ходить не надо вообще.
- Интеграцию с AD с помощью Kerberos и NTLM.
- Строить красивые графики и отчеты, которые не стыдно показать.
- Мульти WAN и отказоустойчивость на базе CARP.

Ну и до кучи он имеет сертификацию ФСТЭК (как я понял, сейчас она в стадии продления) и включен в единый реестр российского ПО, что в некоторых случаях очень важно. Бесплатно можно использовать шлюз для работы с ним до 9-ти пользователей, либо получить 35-ти дневную бесплатную версию без ограничения числа пользователей для теста. В обоих случаях это будут полнофункциональные варианты работы шлюза.

После первого знакомства с продуктом и тестирования основного функционала, у меня осталось положительное впечатление. Я хорошо знаком с вопросом настройки шлюзов и контроля трафика в небольших и средних компаниях, так как много занимался этой темой, когда обслуживал офисы. По запросам руководства настраивал ограничение доступа, предоставлял отчеты и т.д. Дело чаще всего бесполезное, но тем не менее, запросы такие были регулярно.

В комментариях к первой статье я получил некоторое количество негатива в сторону ИКС. Якобы это поделка со сменой лейбла на базе готовых open source наработок. Но по факту, никто так и не привел примера, с помощью какого готового бесплатного продукта можно получить схожий функционал. Да, есть pfsense, но у него, к примеру, нет нормальных отчетов, которые можно показать руководству. LightSquid в данном случае не подходит, так как на его отчеты и самому смотреть не хочется, не то, что показывать кому-то.

В общем, я считаю, что интернет шлюз ИКС неплохой продукт и может быть полезен, поэтому согласился написать по нему очередную статью. Она будет на тему организации VPN туннелей. Эту тему я еще не разбирал, так что будет интересно посмотреть, что и как он умеет делать.

Что нового в ИКС 7.1

Пройдемся кратенько по изменениям новой версии. Итак, что изменилось с выходом ИКС 7.1?

1. Перешли на кодовую базу Freebsd 12.1.
2. Добавили авторизацию пользователей из AD через Kerberos. Раньше только NTLM была.
3. Добавили авторизация по звонку в Captive Portal: в публичной wi-fi сети можно авторизовываться путем звонка на определенный номер.
4. Появилась возможность получить IPSec туннель с оборудованием других вендоров (mikrotik, cisco и пр.).
5. Прочие небольшие доработки и исправления, в том числе на основе запросов клиентов.

Более подробный список изменений можно посмотреть на отдельной странице. Тестированием работы подключения к VPN туннелям ipsec на базе микротиков займемся далее. Тема актуальная, так как микротики последнее время очень активно используют организации.

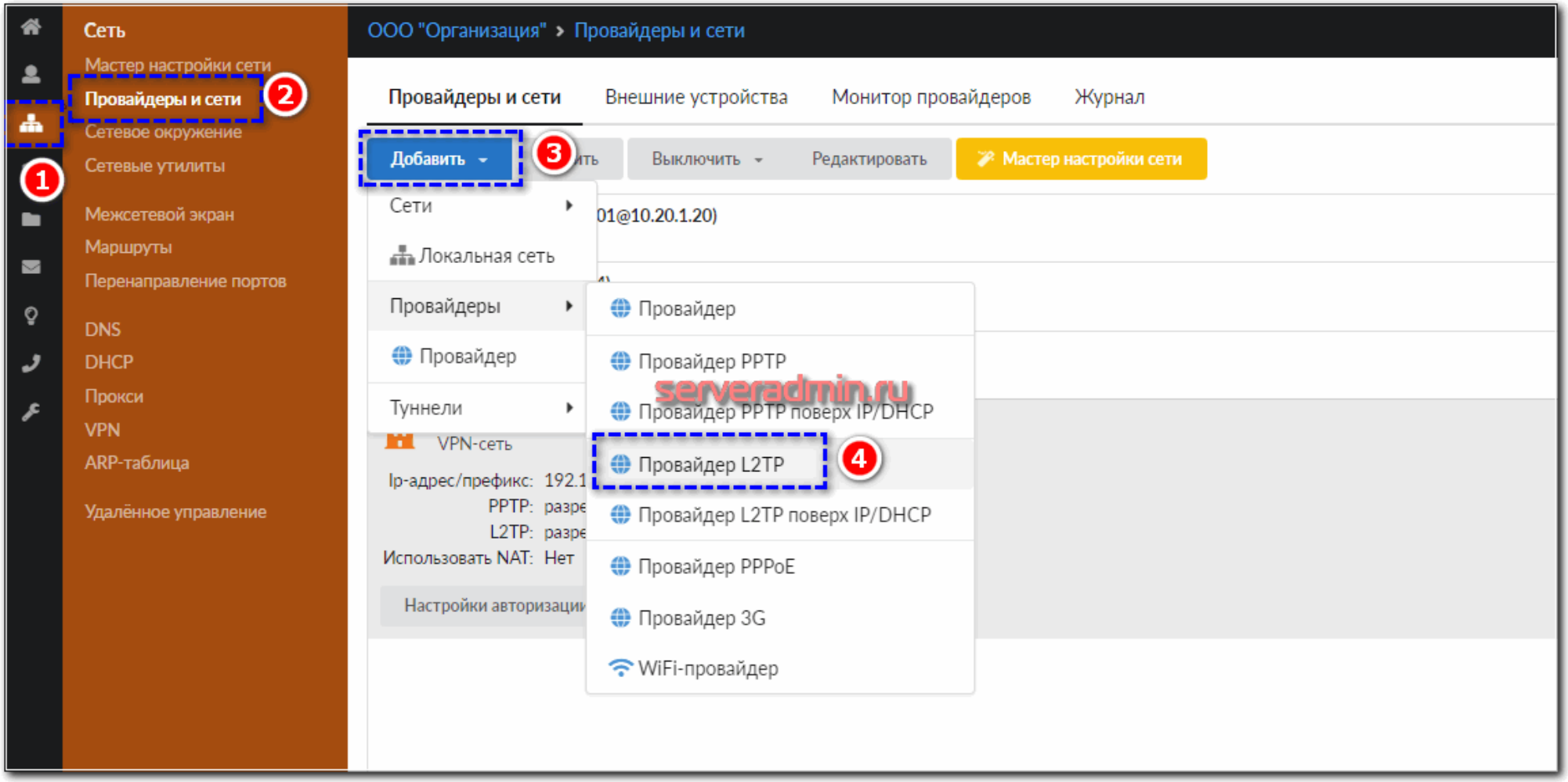
Подключение к стороннему IPSEC туннелю

Допустим, у вас есть какая-то удаленная локальная сеть (192.168.88.0/24), которую обслуживает Mikrotik с настроенным l2tp + ipsec. И вам нужно подключиться к нему, чтобы ходить в эту сеть. Настраивается все достаточно просто, наглядно и логично. Хотя я и делал это первый раз, все получилось сразу без чтения документации :) Единственное, не сразу нашел, где собственно добавлять новое подключнние к vpn.

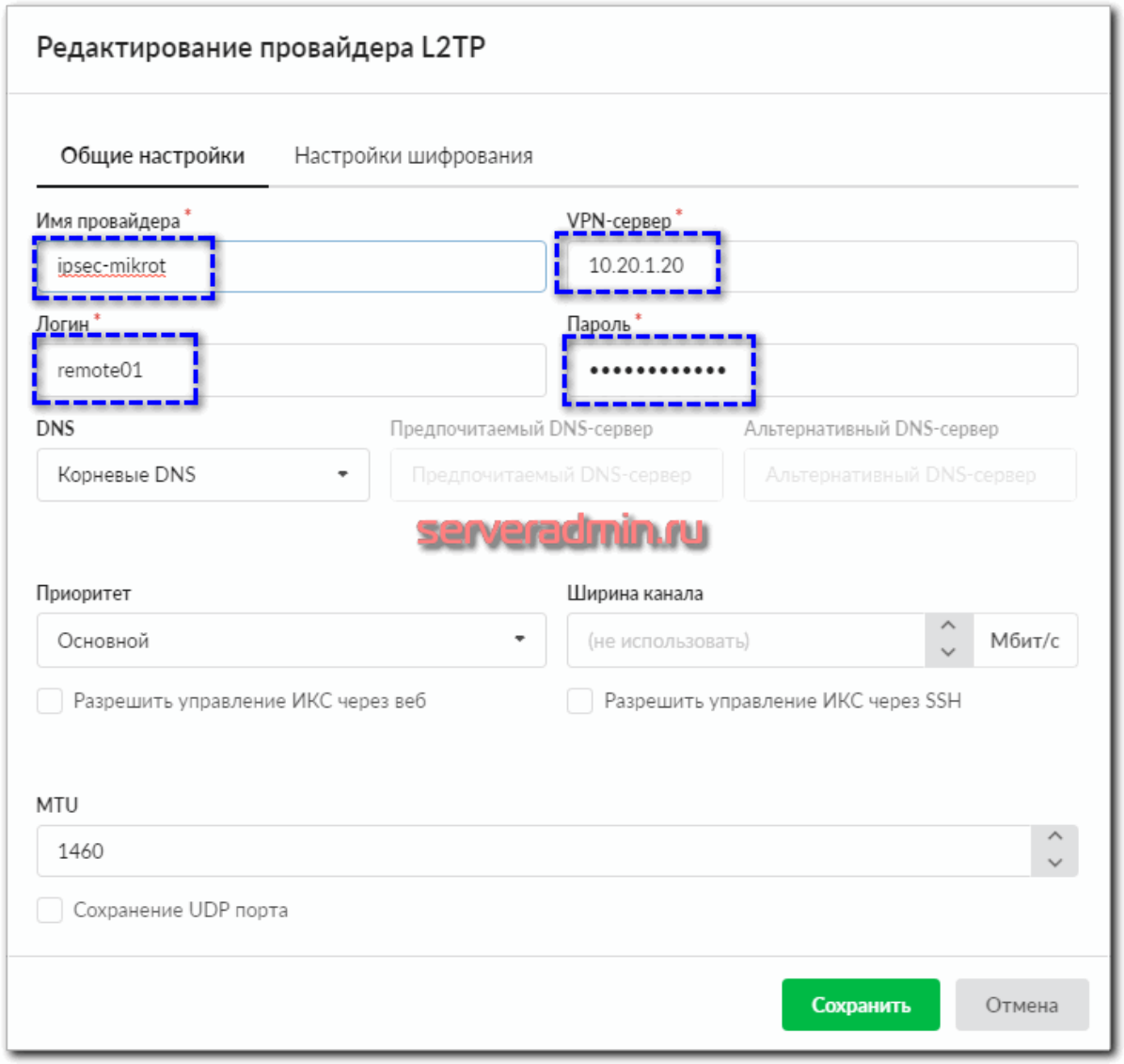
Логика объединения сетей с помощью VPN одинакова везде. Нам нужно:

1. Подключиться к VPN.
2. Настроить маршруты.
3. Настроить firewall.
4. Проверить подключение.

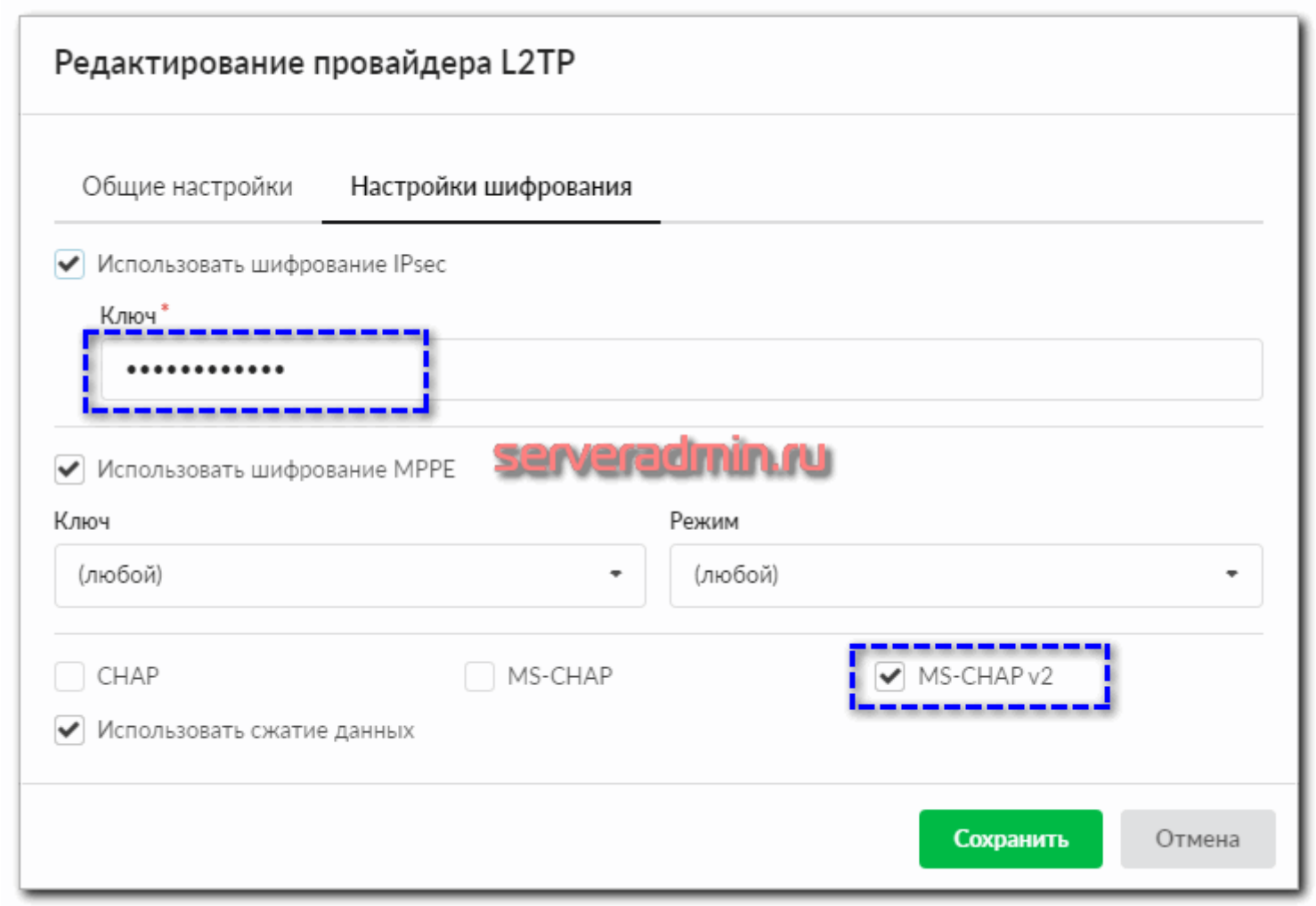
Начинаем с настройки подключения. Идем в раздел **Сеть -> Провайдеры и сети -> Добавить -> Провайдер l2tp**. На этом моменте я немного залип, так как не понял, что надо добавить именно провайдера. Я же не провайдера подключаю, а удаленный филиал.



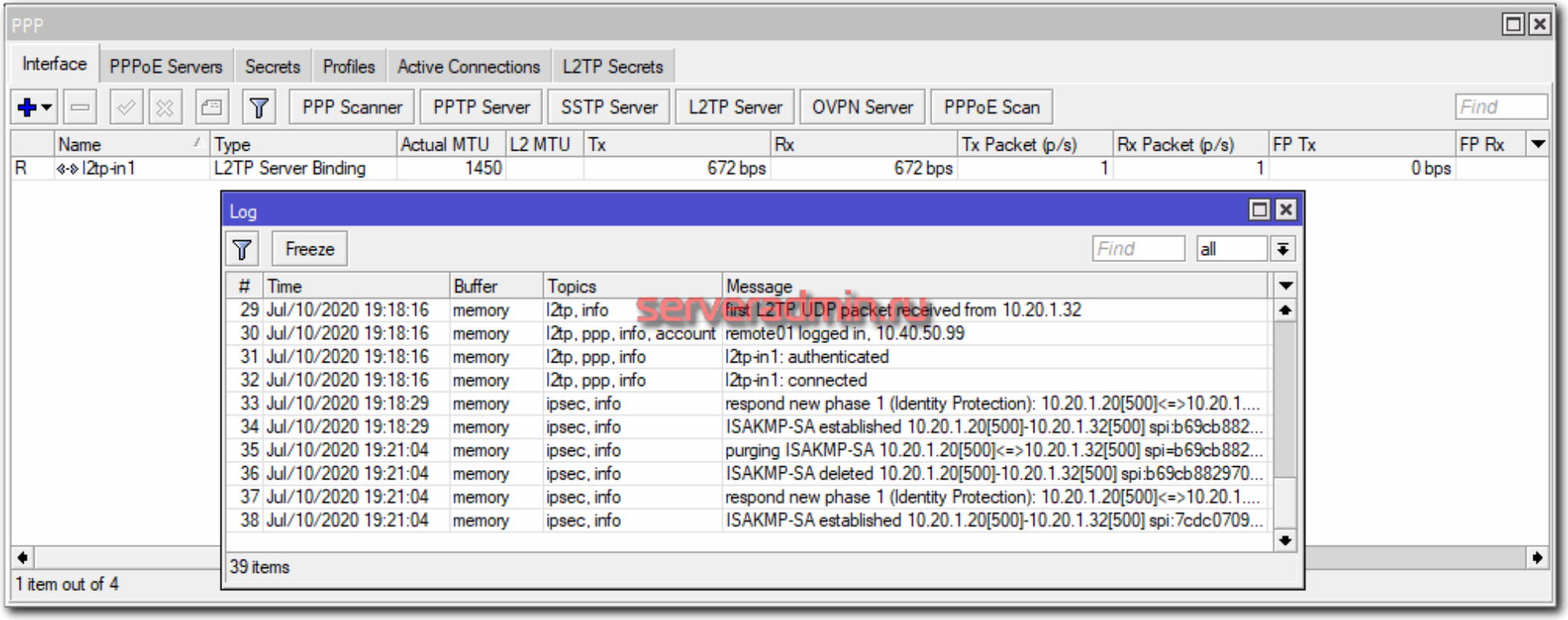
Дальше заполняем необходимые параметры. Для Mikrotik достаточно следующих.


Редактирование провайдера L2TP
Общие настройки
Настройки шифрования
Имя провайдера *
ipsec-mikrot
VPN-сервер *
10.20.1.20
Логин *
remote01
Пароль *
••••••••••••
DNS
Корневые DNS
Предпочитаемый DNS-сервер
Альтернативный DNS-сервер
serveradmin.ru
Приоритет
Основной
Ширина канала
(не использовать)
Мбит/с
Разрешить управление ИКС через веб
Разрешить управление ИКС через SSH
MTU
1460
Сохранение UDP порта
Сохранить
Отмена

Если настроен ipsec, указываем его пароль на соседней вкладке.

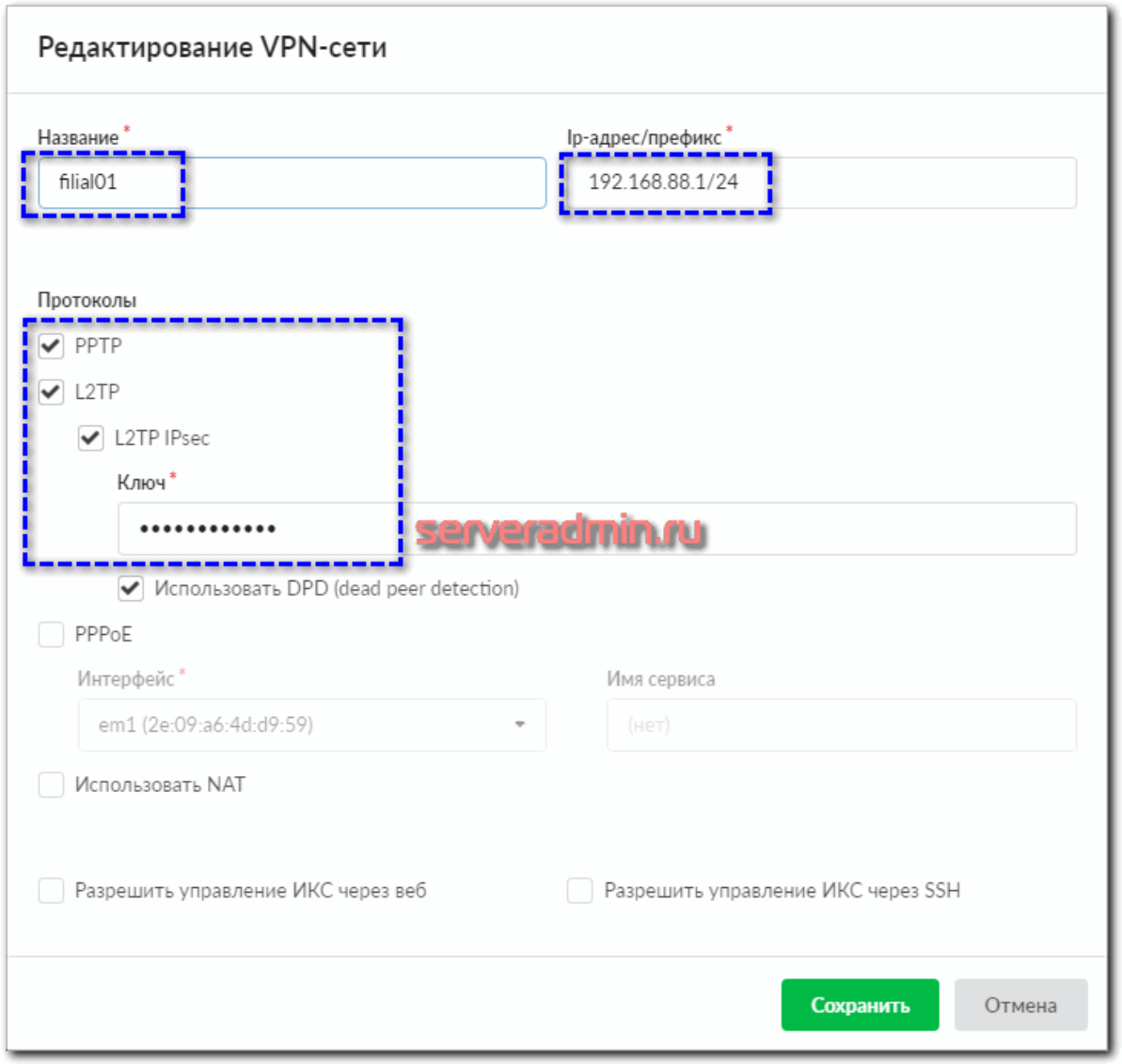


После сохранения настроек сразу же идет подключение. На микротике вижу его.

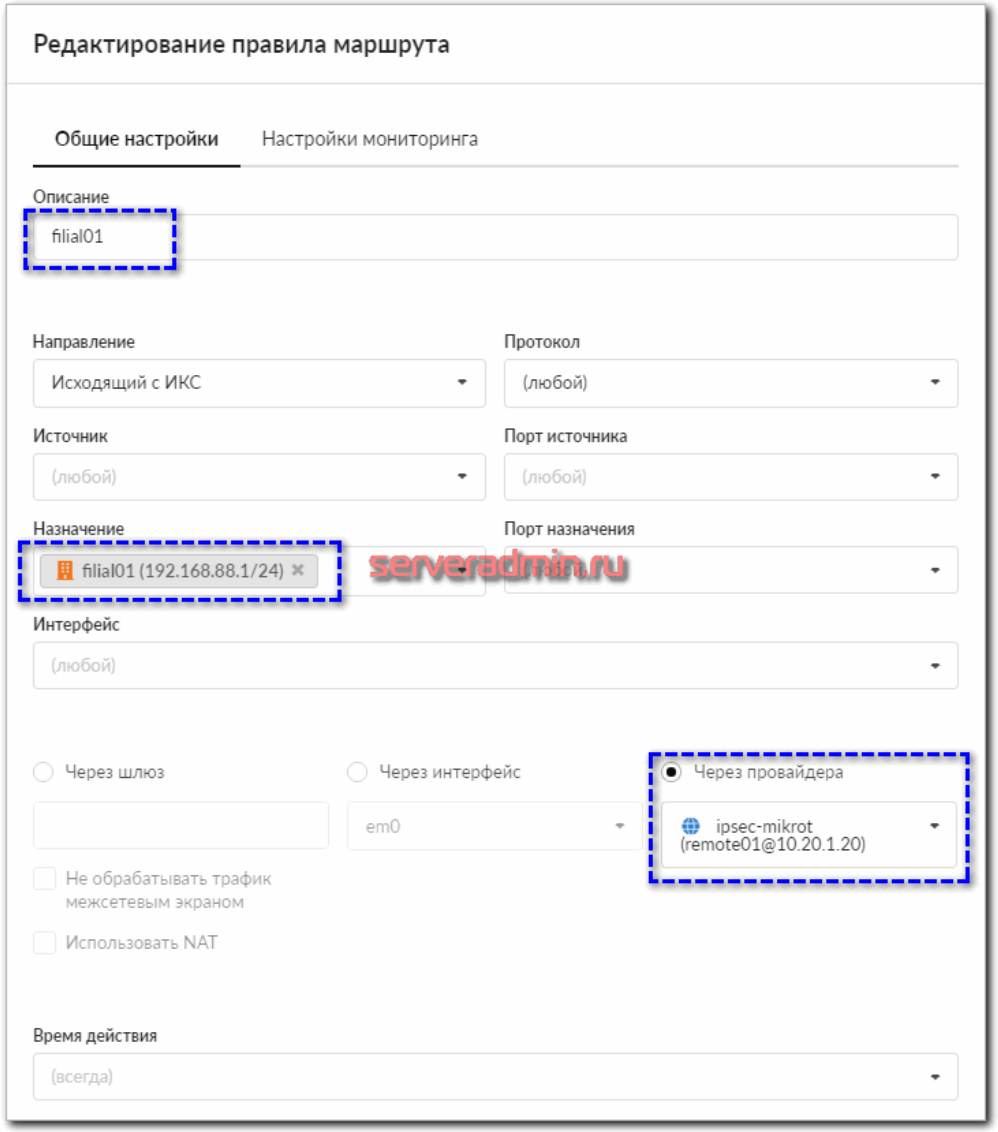


Дальше важный момент, на котором постоянно зависают новички, настраивающие VPN. Они не понимают, как работает маршрутизация и ожидают, что теперь они сразу же смогут обращаться в удаленную сеть, которую подключили через VPN. В данном случае нет. Ваши запросы будут приходить на дефолтный шлюз, а он не будет знать, что с ними делать. Чтобы он понимал, что их надо отправлять в vpn туннель, надо создать отдельный маршрут для этого.

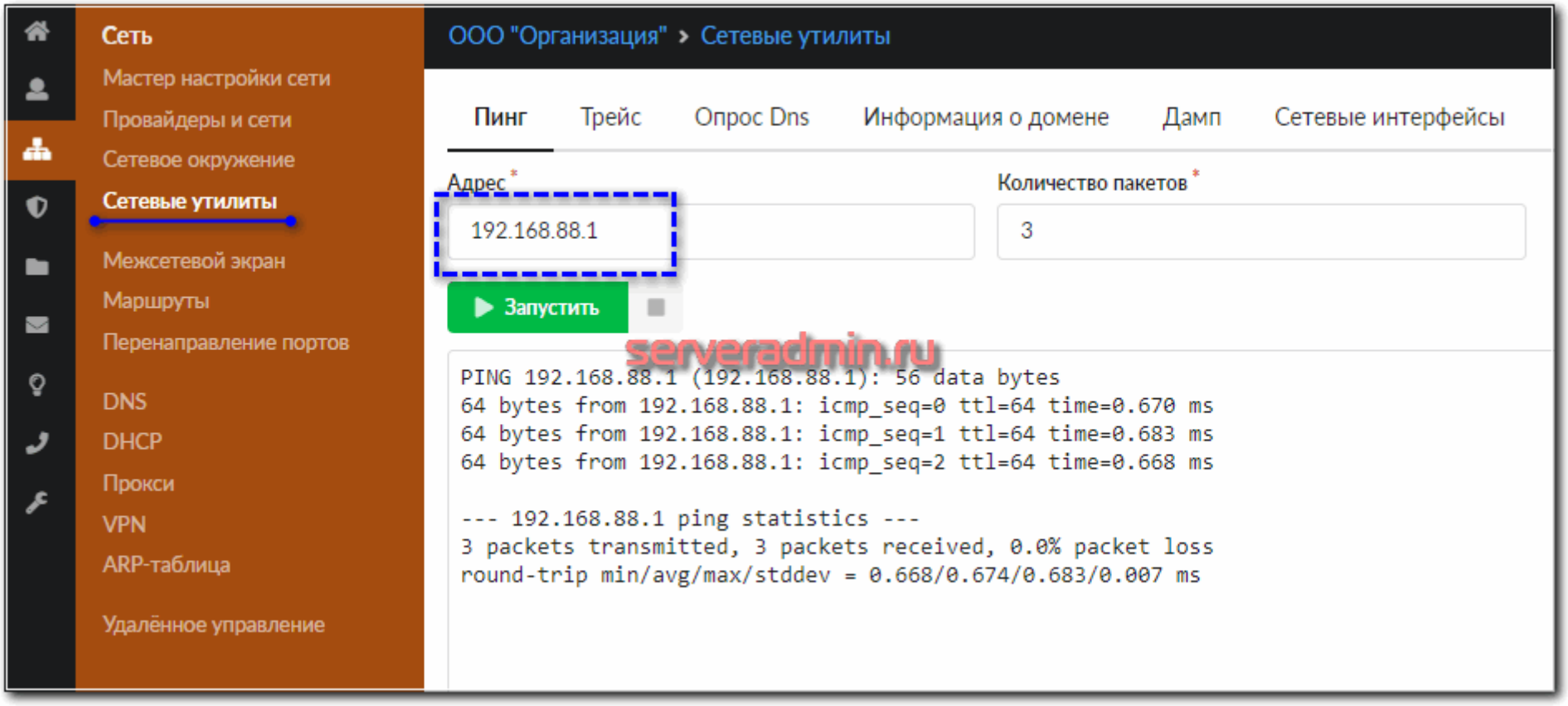
В шлюзе ИКС можно создавать готовые сущности, а потом ими оперировать в настройках. Это удобно и наглядно. Создадим сущность VPN-сеть и назовем ее filial01. Для этого здесь же, в разделе **Провайдеры и сети** создаем VPN-сеть.


Редактирование VPN-сети
Название *
filial01
Ip-адрес/префикс *
192.168.88.1/24
Протоколы
PPTP
L2TP
L2TP IPsec
Ключ *
••••••••••••
serveradmin.ru
Использовать DPD (dead peer detection)
PPPoE
Интерфейс *
em1 (2e:09:a6:4d:d9:59)
Имя сервиса
(нет)
Использовать NAT
Разрешить управление ИКС через веб
Разрешить управление ИКС через SSH
Сохранить
Отмена

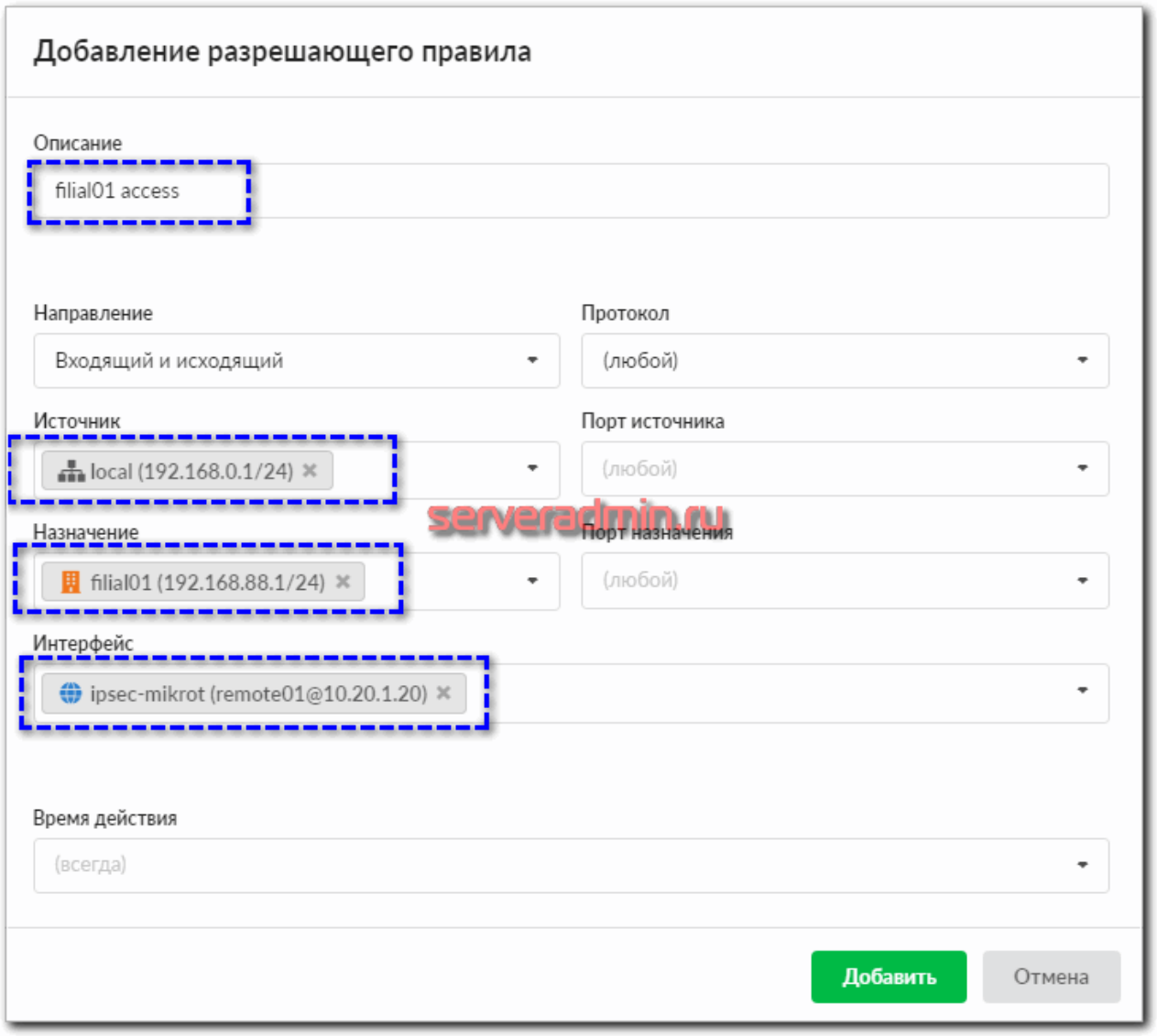
Отправляемся в раздел **Маршруты** и добавляем новый маршрут.


Редактирование правила маршрута
Общие настройки
Настройки мониторинга
Описание
filial01
Направление
Исходящий с ИКС
Протокол
(любой)
Источник
(любой)
Порт источника
(любой)
Назначение
filial01 (192.168.88.1/24)
Порт назначения
serveradmin.ru
Интерфейс
(любой)
Через шлюз
Через интерфейс
Через провайдера
em0
ipsec-mikrot (remote01@10.20.1.20)
Не обрабатывать трафик межсетевым экраном
Использовать NAT
Время действия
(всегда)

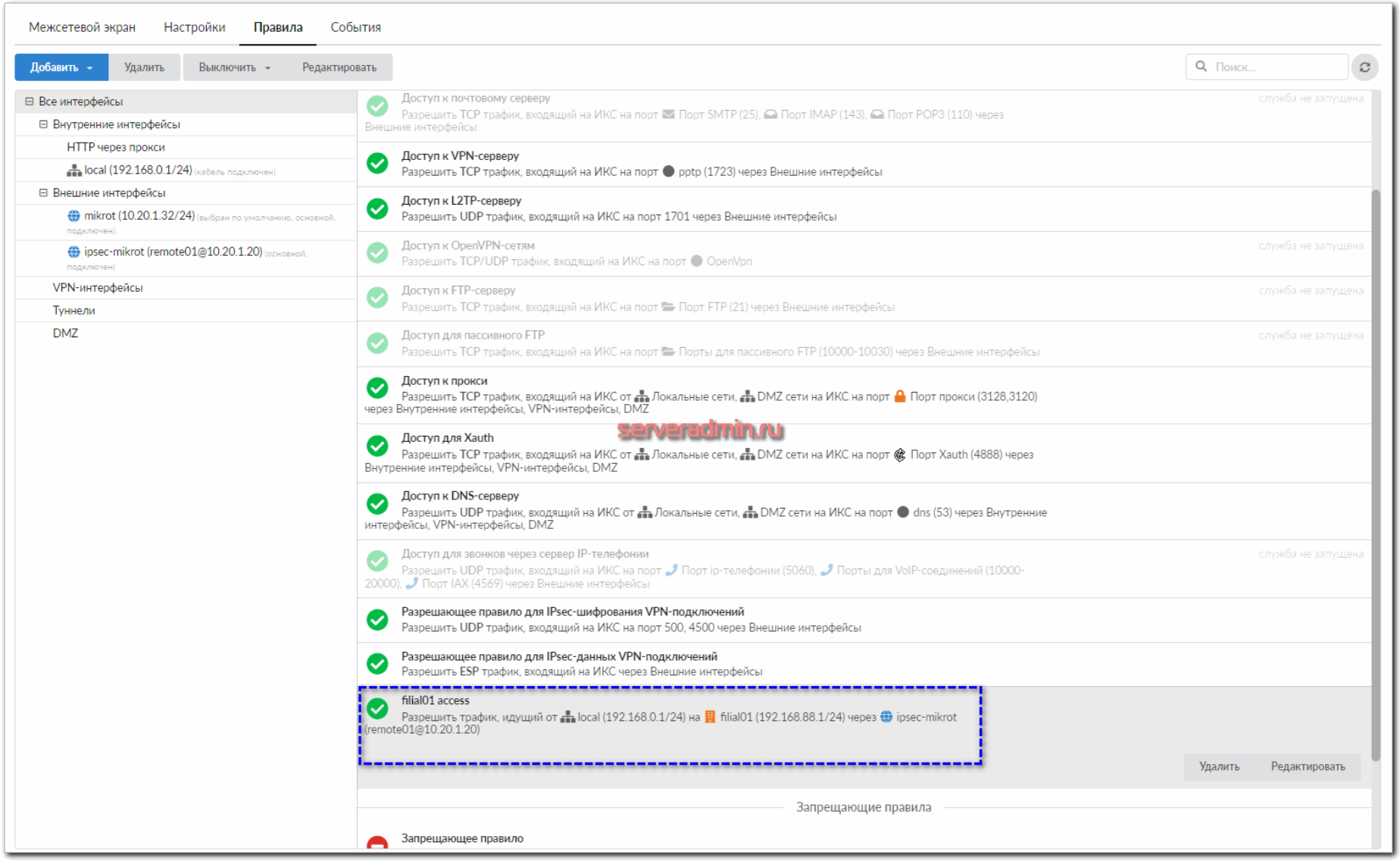
После этого можно уже проверить связь, так как в фаерволе по умолчанию разрешены пинги. Идем в раздел **Сетевые утилиты** и пингуем один из адресов из удаленной подсети.



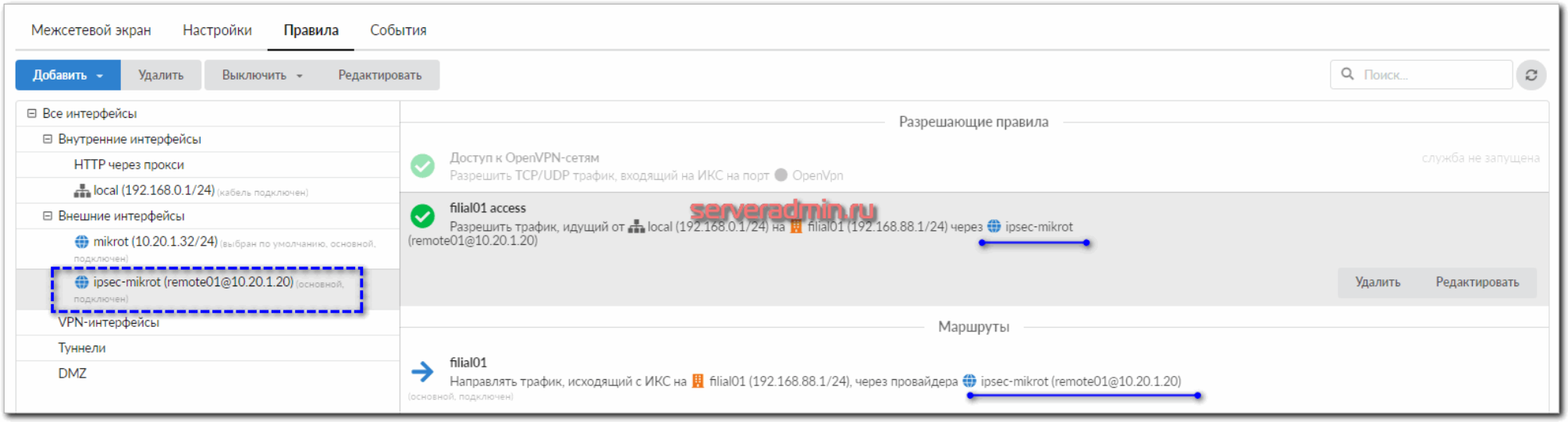
Далее нужно добавить разрешающее правило в фаерволе для vpn трафика. Можете разрешить весь трафик или указать что-то конкретное. На ваше усмотрение. Интерфейс наглядный и понятный.


Добавление разрешающего правила
Описание
filial01 access
Направление
Входящий и исходящий
Протокол
(любой)
Источник
local (192.168.0.1/24)
Порт источника
(любой)
serveradmin.ru
Назначение
filial01 (192.168.88.1/24)
Порт назначения
(любой)
Интерфейс
ipsec-mikrot (remote01@10.20.1.20)
Время действия
(всегда)
Добавить
Отмена

Новое правило появляется в списке.

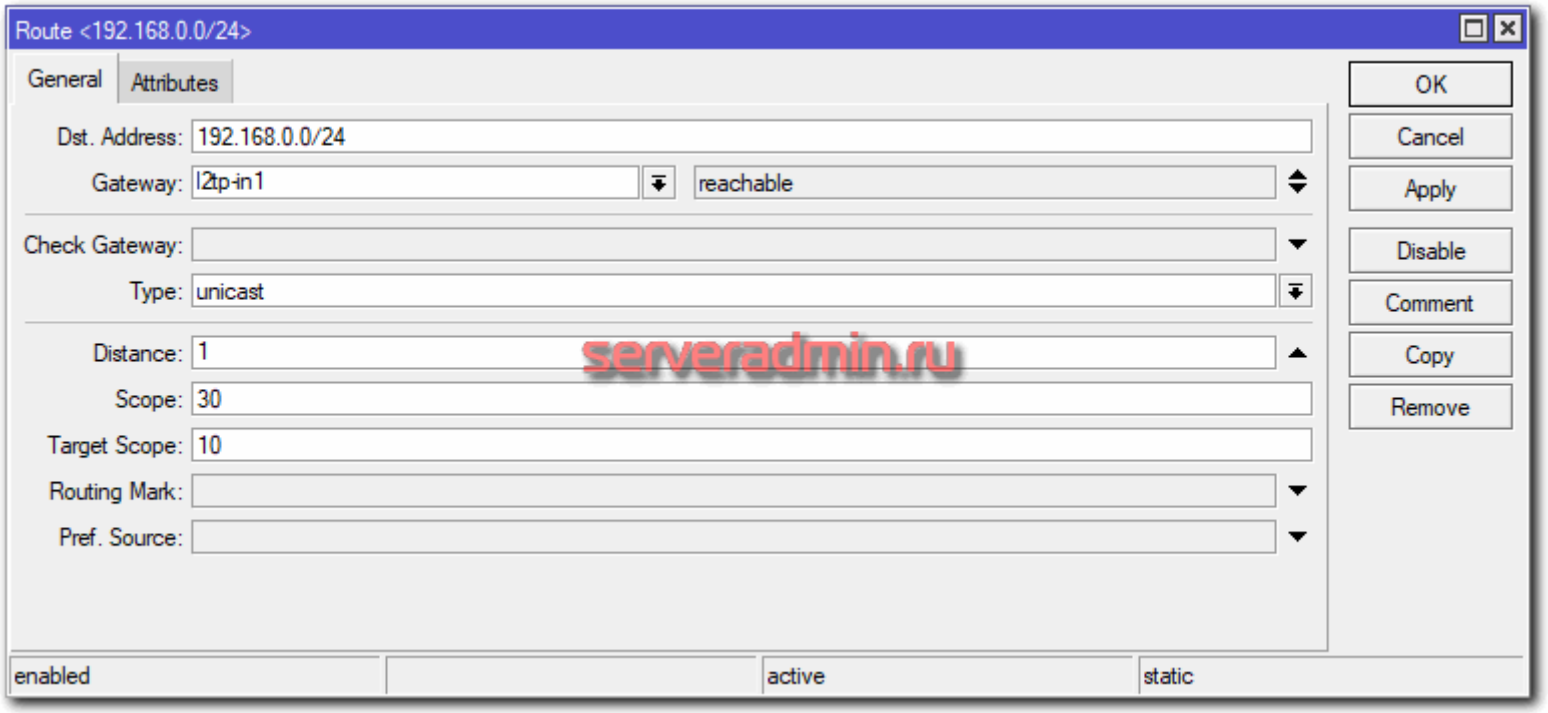

Межсетевой экран
Настройки
Правила
События
Добавить
Удалить
Выключить
Редактировать
Поиск...
Все интерфейсы
Внутренние интерфейсы
HTTP через прокси
local (192.168.0.1/24) (кабель подключен)
Внешние интерфейсы
mikrot (10.20.1.32/24) (выбран по умолчанию, основной, подключен)
ipsec-mikrot (remote01@10.20.1.20) (основной, подключен)
VPN-интерфейсы
Туннели
DMZ
Доступ к почтовому серверу
Разрешить TCP трафик, входящий на ИКС на порт Порт SMTP (25), Порт IMAP (143), Порт POP3 (110) через Внешние интерфейсы
служба не запущена
Доступ к VPN-серверу
Разрешить TCP трафик, входящий на ИКС на порт pptp (1723) через Внешние интерфейсы
Доступ к L2TP-серверу
Разрешить UDP трафик, входящий на ИКС на порт 1701 через Внешние интерфейсы
Доступ к OpenVPN-сетям
Разрешить TCP/UDP трафик, входящий на ИКС на порт OpenVpn
служба не запущена
Доступ к FTP-серверу
Разрешить TCP трафик, входящий на ИКС на порт Порт FTP (21) через Внешние интерфейсы
служба не запущена
Доступ для пассивного FTP
Разрешить TCP трафик, входящий на ИКС на порт Порты для пассивного FTP (10000-10030) через Внешние интерфейсы
служба не запущена
Доступ к прокси
Разрешить TCP трафик, входящий на ИКС от Локальные сети, DMZ сети на ИКС на порт Порт прокси (3128,3120) через Внутренние интерфейсы, VPN-интерфейсы, DMZ
serveradmin.ru
Доступ для Xauth
Разрешить TCP трафик, входящий на ИКС от Локальные сети, DMZ сети на ИКС на порт Порт Xauth (4888) через Внутренние интерфейсы, VPN-интерфейсы, DMZ
Доступ к DNS-серверу
Разрешить UDP трафик, входящий на ИКС от Локальные сети, DMZ сети на ИКС на порт dns (53) через Внутренние интерфейсы, VPN-интерфейсы, DMZ
Доступ для звонков через сервер IP-телефонии
Разрешить UDP трафик, входящий на ИКС на порт Порт ip-телефонии (5060), Порты для VoIP-соединений (10000-20000), Порт IAX (4569) через Внешние интерфейсы
служба не запущена
Разрешающее правило для IPsec-шифрования VPN-подключений
Разрешить UDP трафик, входящий на ИКС на порт 500, 4500 через Внешние интерфейсы
Разрешающее правило для IPsec-данных VPN-подключений
Разрешить ESP трафик, входящий на ИКС через Внешние интерфейсы
filial01 access
Разрешить трафик, идущий от local (192.168.0.1/24) на filial01 (192.168.88.1/24) через ipsec-mikrot (remote01@10.20.1.20)
Удалить
Редактировать
Запрещающие правила
Запрещающее правило

Вообще, мне понравился интерфейс управления правилами фаервола. Пожалуй, это один из наиболее удобных и наглядных интерфейсов, которые мне доводилось видеть. Слева список сетевых сущностей в виде интерфейсов и сетей. При нажатии на какую-то сущность, появляются все правила и маршруты, связанные с ней.



Удобно разбираться в сложных конфигурациях с десятками правил. При этом, все настраивается через веб интерфейс. Не надо лазить в консоль. Под капотом pf и ipfw.

Напоследок добавлю, что для того, чтобы связь между сетями через vpn работала, на удаленном микротике так же нужно добавить маршрут, который будет указывать, что трафик для сети 192.168.0.0/24 должен идти через l2tp туннель.



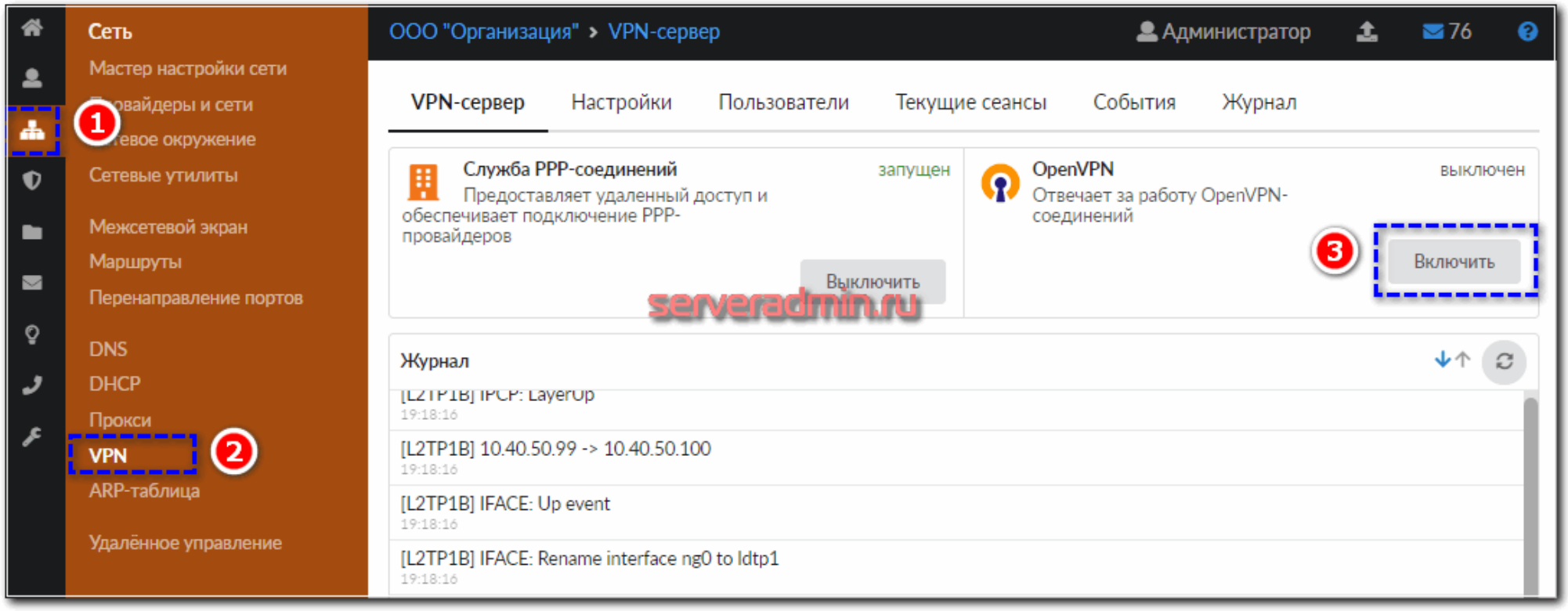
И не забыть про firewall. Надо так же разрешить нужный трафик. Не буду на этом останавливаться в рамках данной статьи.

Разобрал данный кейс просто чтобы продемонстрировать вам интерфейс управления. Мне лично он понравился. Удобно и наглядно. Хотя может это только мое восприятие, так как я хорошо ориентируюсь в подобных шлюзах. Возможно новичку все будет не так очевидно и понятно.

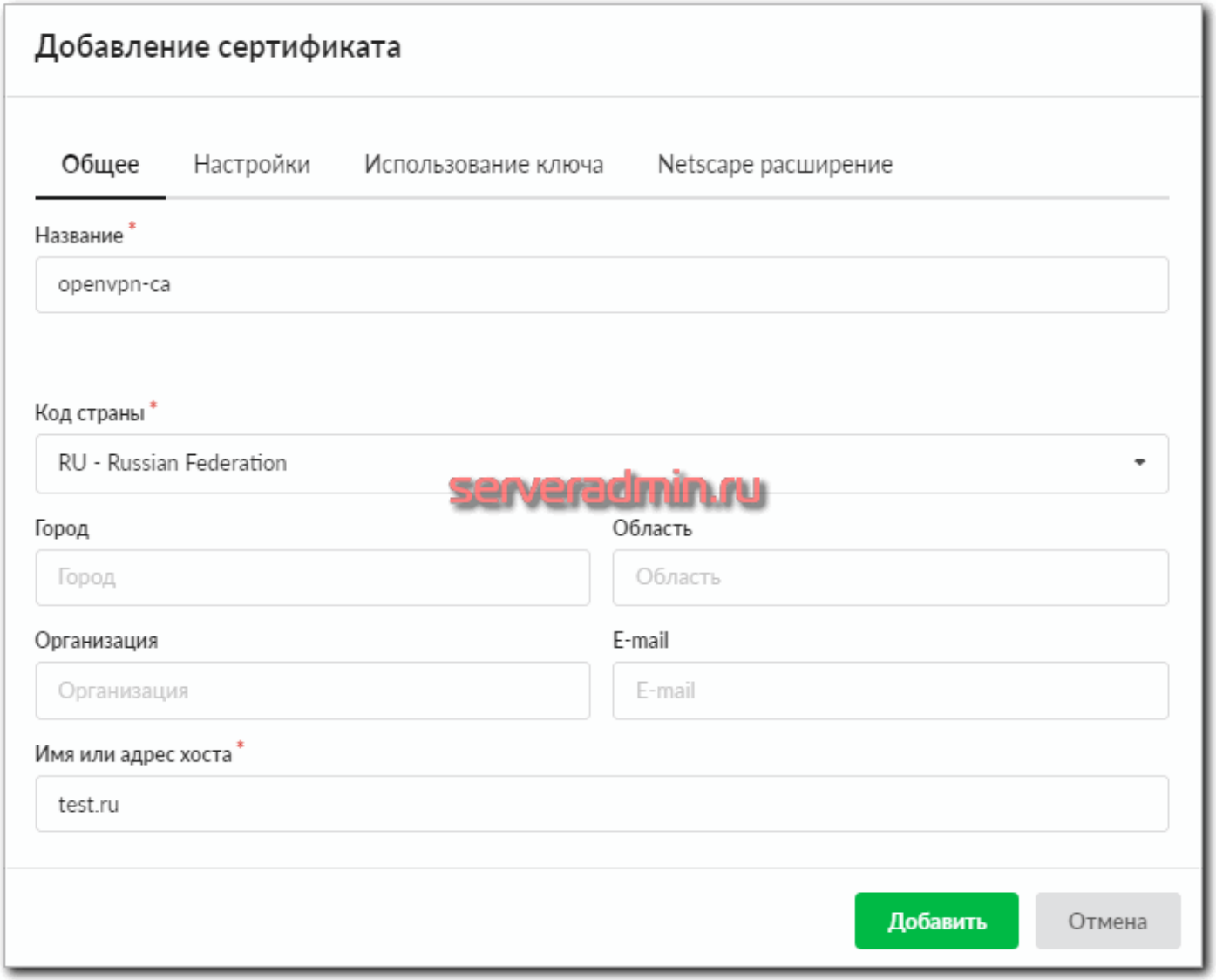
Настройка своего VPN сервера

Теперь разберу еще один полезный, на мой взгляд, кейс. Так как ИКС бесплатен для 8-ми пользователей, его можно использовать как личный vpn сервер с удобным веб интерфейсом. Я покажу это на примере настройки OpenVPN сервера.

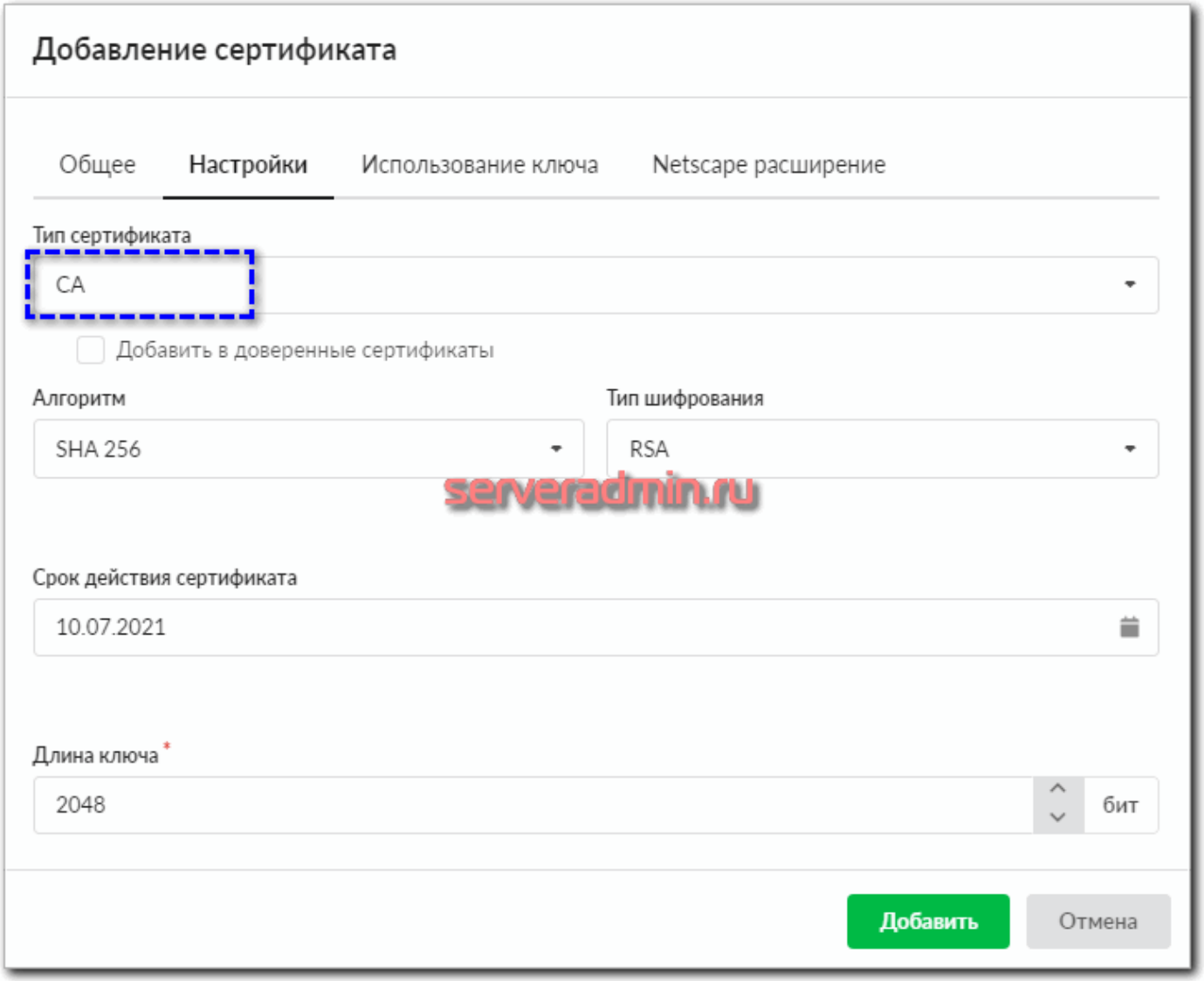
Идем в раздел **VPN** и запускаем OpenVPN.



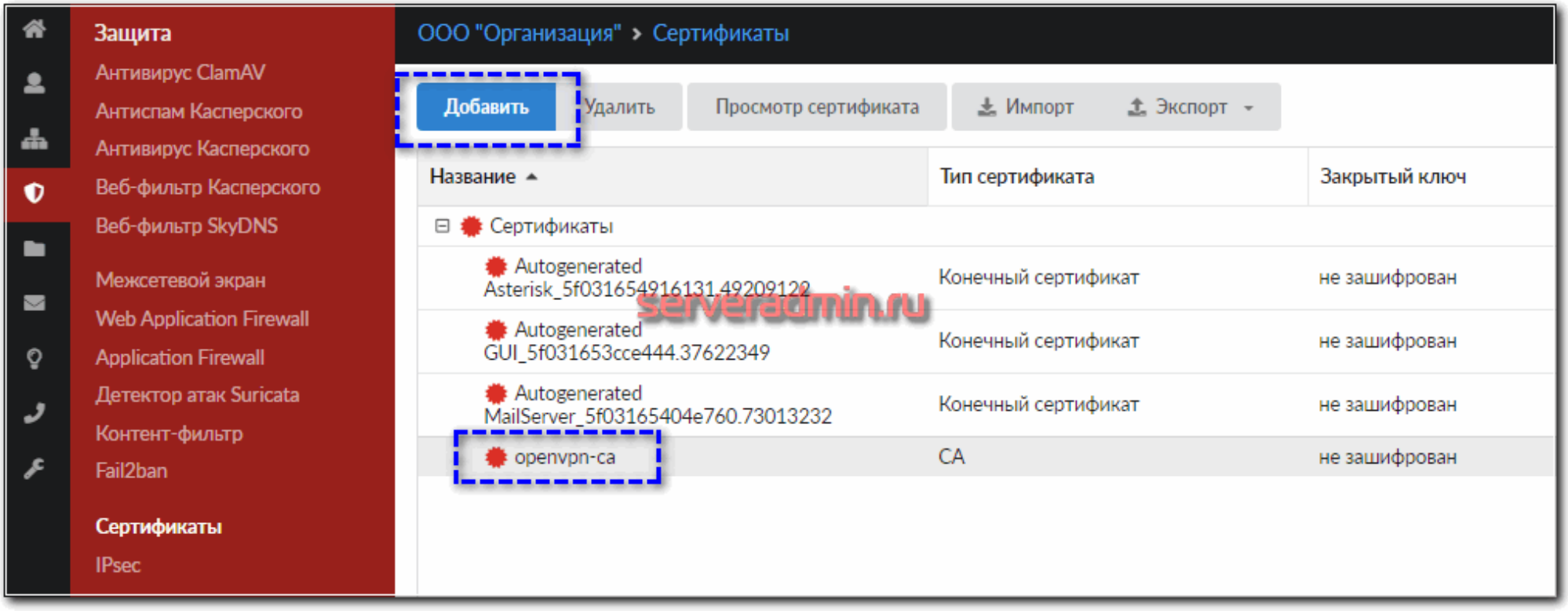
Нам надо выпустить сертификаты для работы openvpn. Для этого идем в раздел **Защита -> Сертификаты** и добавляем новый.


Добавление сертификата
Общее
Настройки
Использование ключа
Netscape расширение
Название *
openvpn-ca
Код страны *
RU - Russian Federation
serveradmin.ru
Город
Область
Город
Область
Организация
E-mail
Организация
E-mail
Имя или адрес хоста *
test.ru
Добавить
Отмена

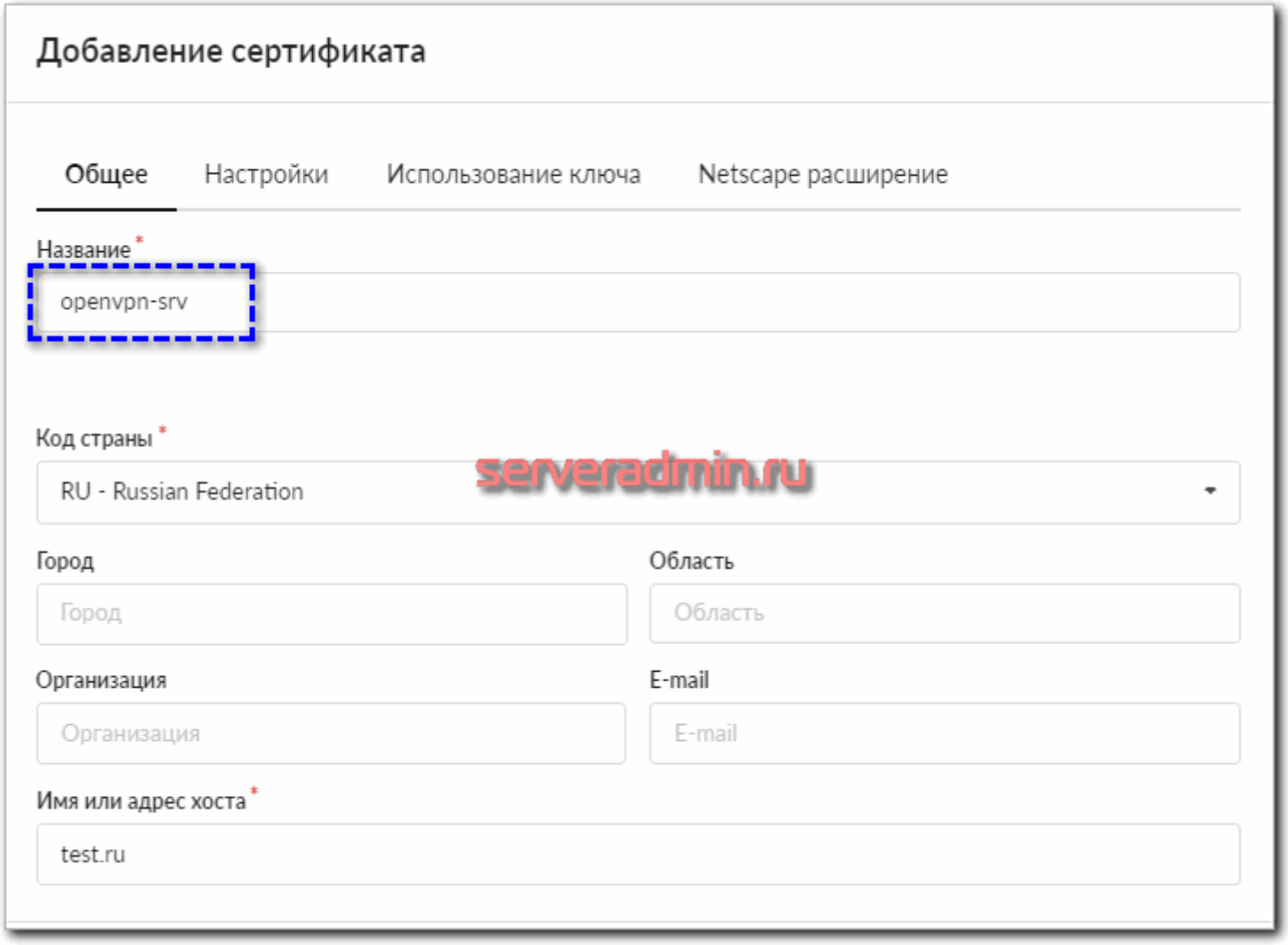
Настройки можно оставить дефолтными, только название указать. И обязательно на вкладке *Настройки* указать, что это CA сертификат.


Добавление сертификата
Общее
Настройки
Использование ключа
Netscape расширение
Тип сертификата
CA
Добавить в доверенные сертификаты
Алгоритм
SHA 256
Тип шифрования
RSA
serveradmin.ru
Срок действия сертификата
10.07.2021
Длина ключа *
2048
бит
Добавить
Отмена

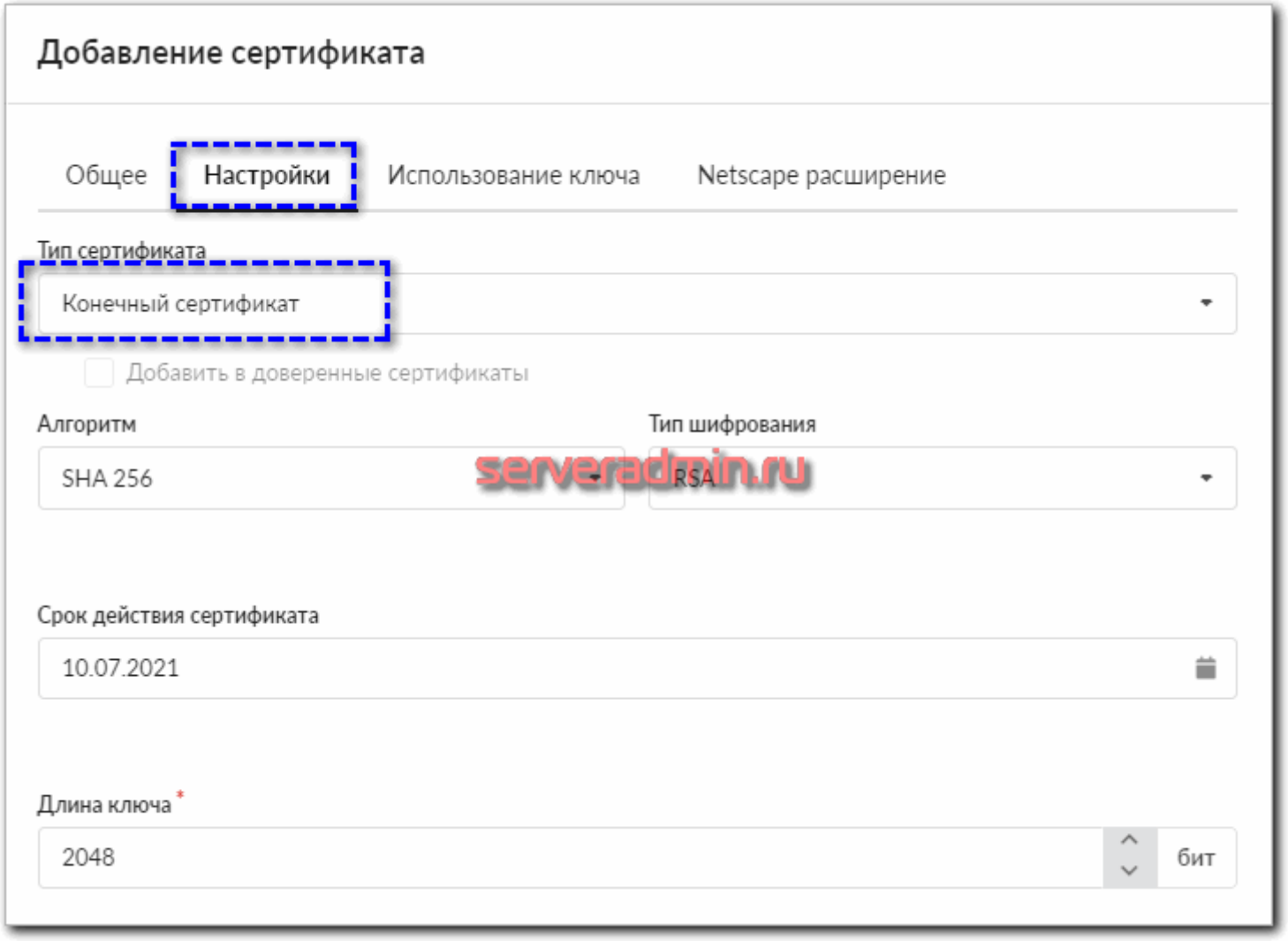
Рекомендую срок действия подольше поставить, чтобы потом не заниматься перевыпуском. После создания CA сертификата, надо добавить сертификат самого сервера. Для этого выбираем созданный сертификат и нажимаем Добавить.



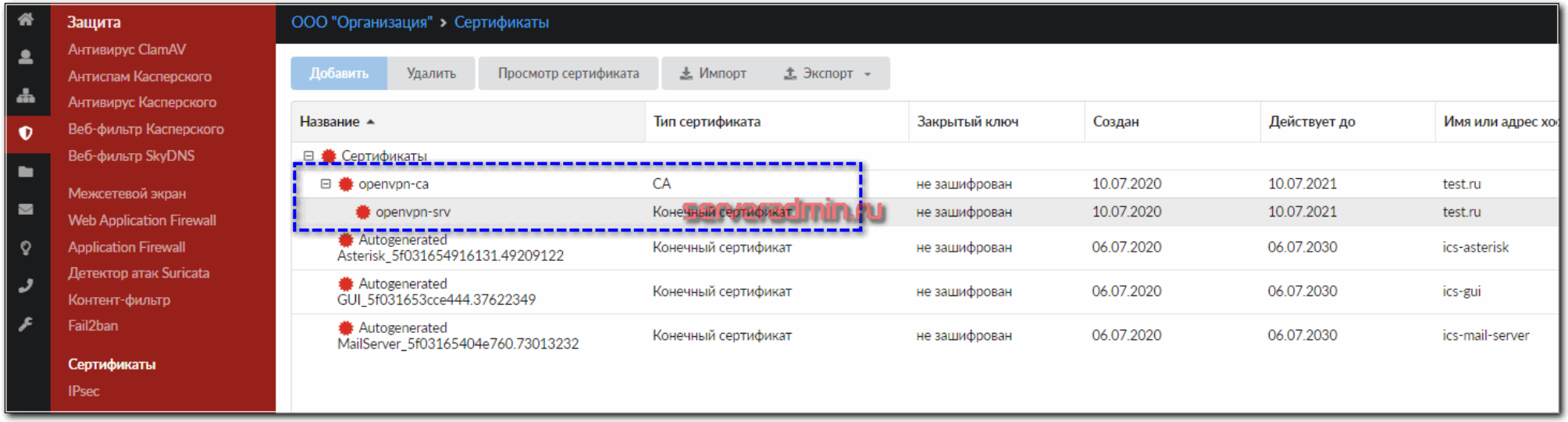
Здесь тоже можно все дефолтное оставить, только поменяйте *Имя или адрес хоста* на что-то отличное от значения CA, иначе openvpn будет ругаться на сертификат при подключении. У меня на скриншоте это не сделано.



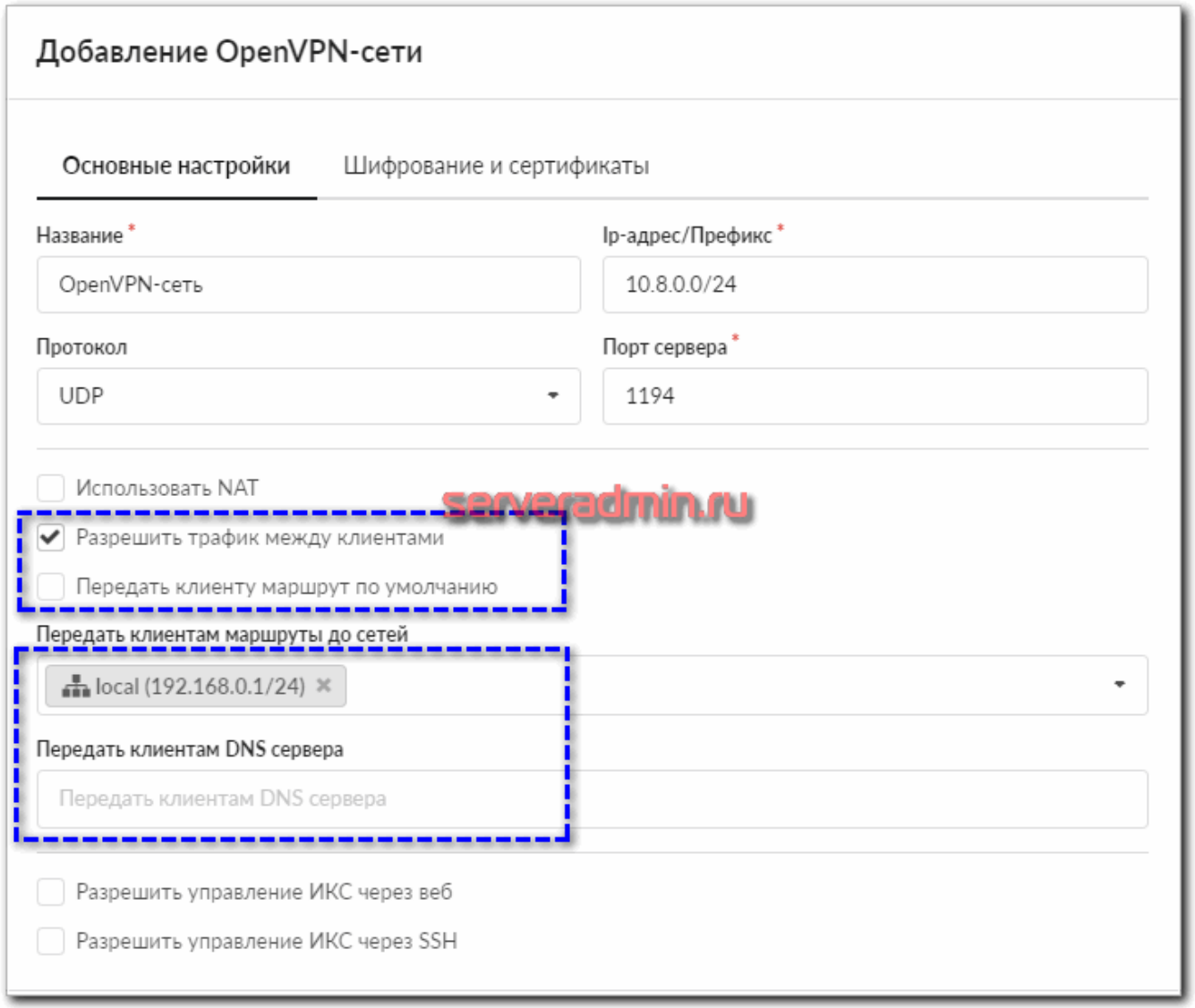
На вкладке *Настройки* обязательно указать, что это *Конечный сертификат*.



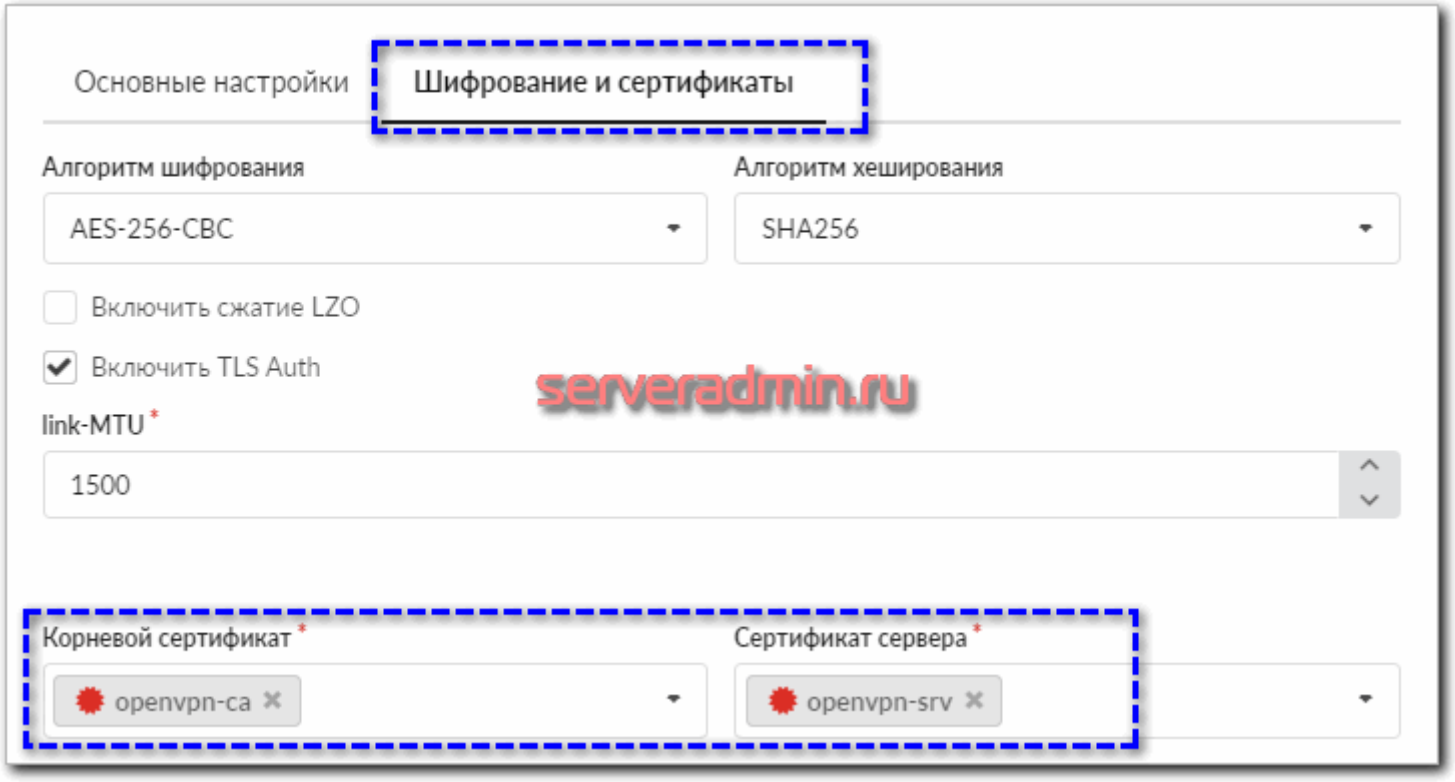
Должно получиться вот так - один сертификат за другим.



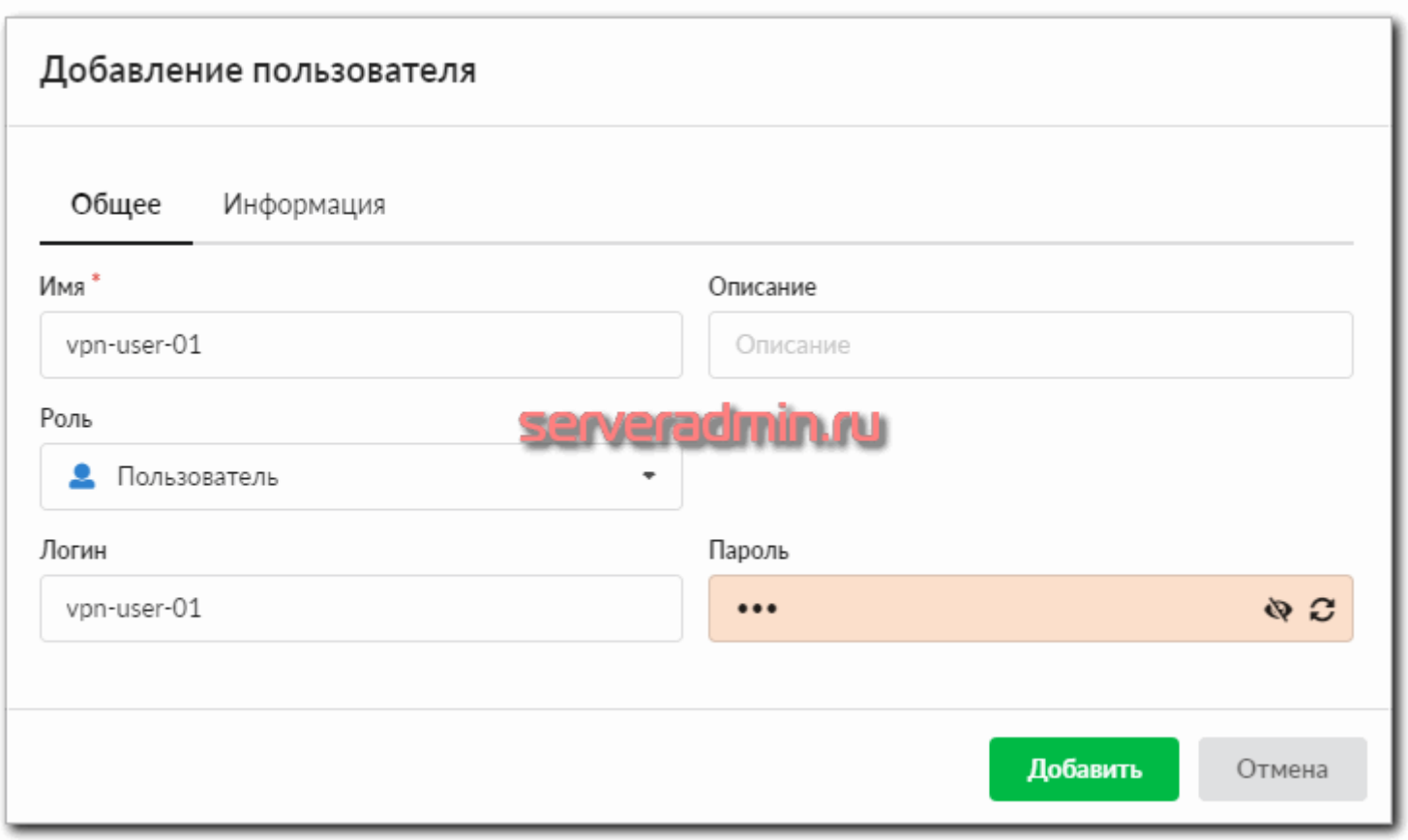
Идем в **Провайдеры и сети** и добавляем Openvpn-сеть.



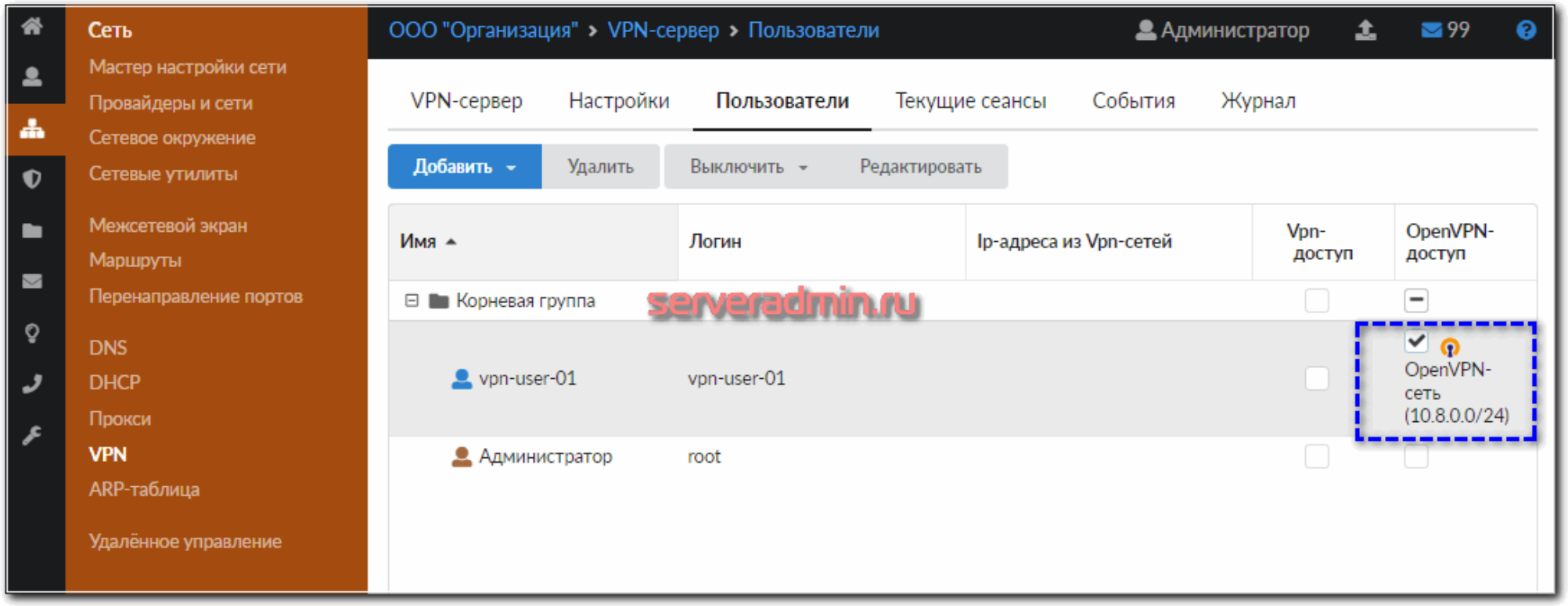
Вам доступен весь основной функционал Openvpn, за который я его люблю. Можете заменять пользователю дефолтный шлюз, прокидывать необходимые маршруты и dns сервера, разрешать трафик между клиентами. На вкладке *Шифрование и сертификаты* укажите созданные ранее сертификаты.



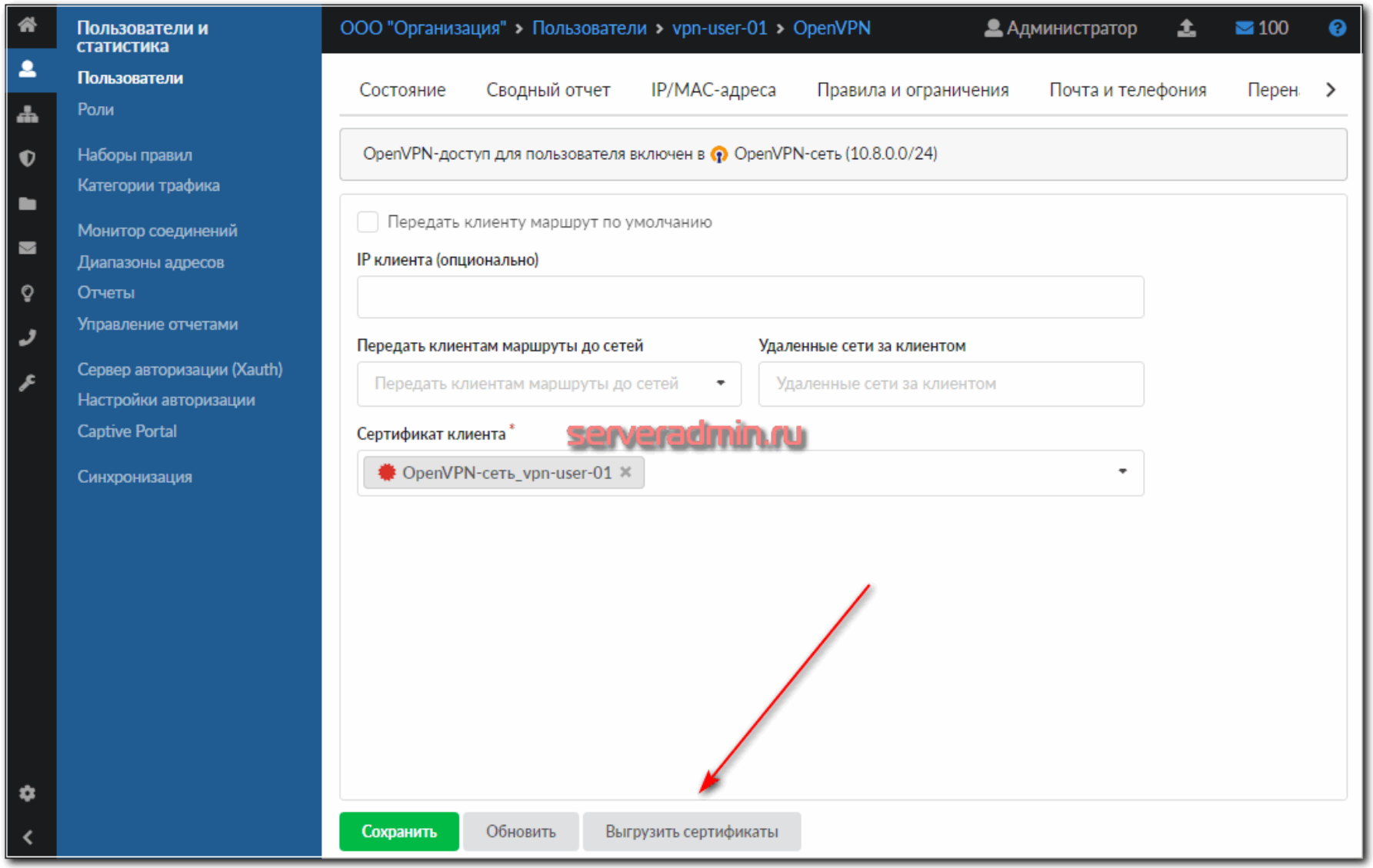
Возвращаемся в раздел VPN и добавляем пользователя.



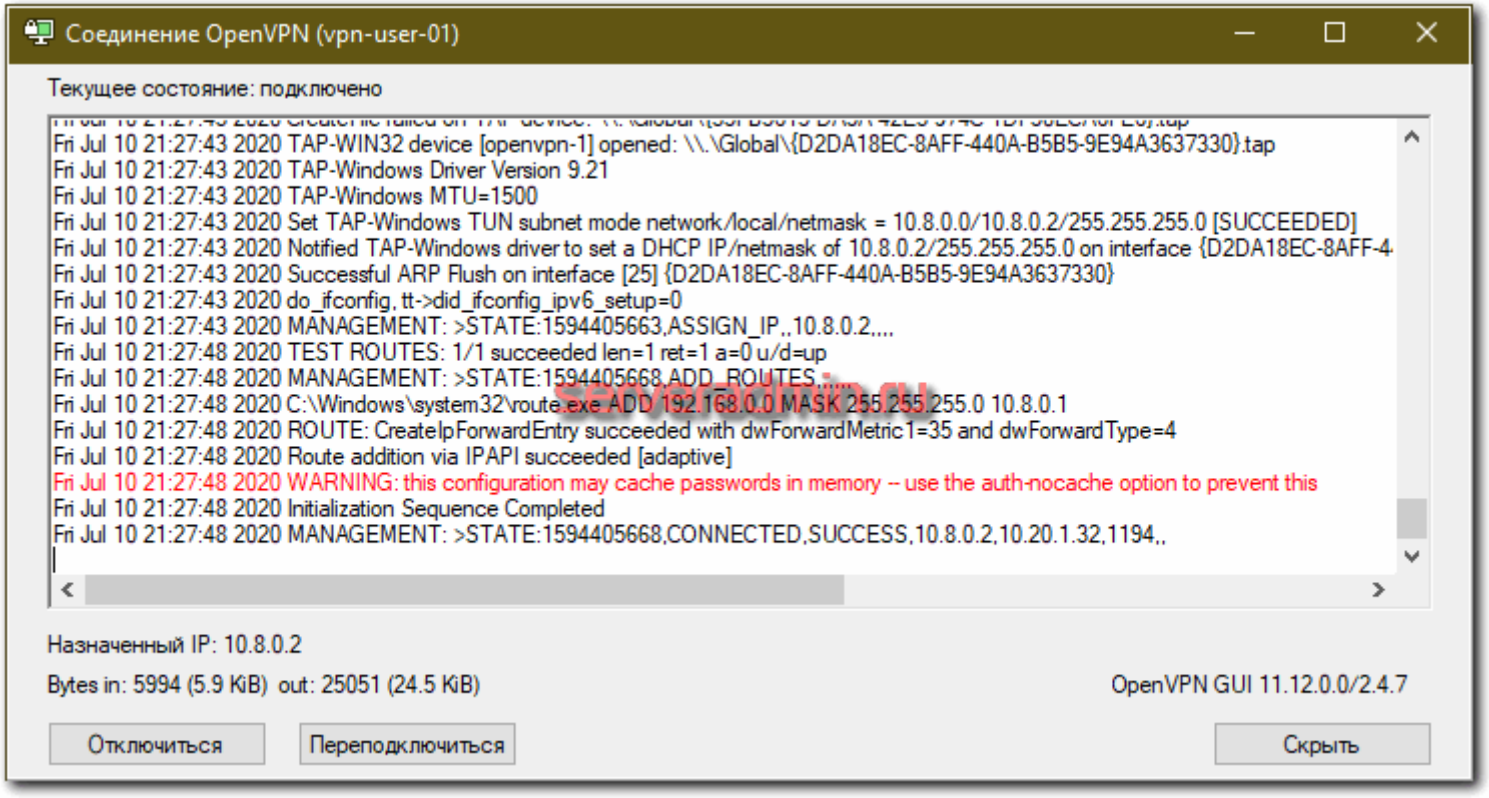
Разрешаем ему OpenVPN доступ и указываем созданную ранее OpenVPN-сеть.



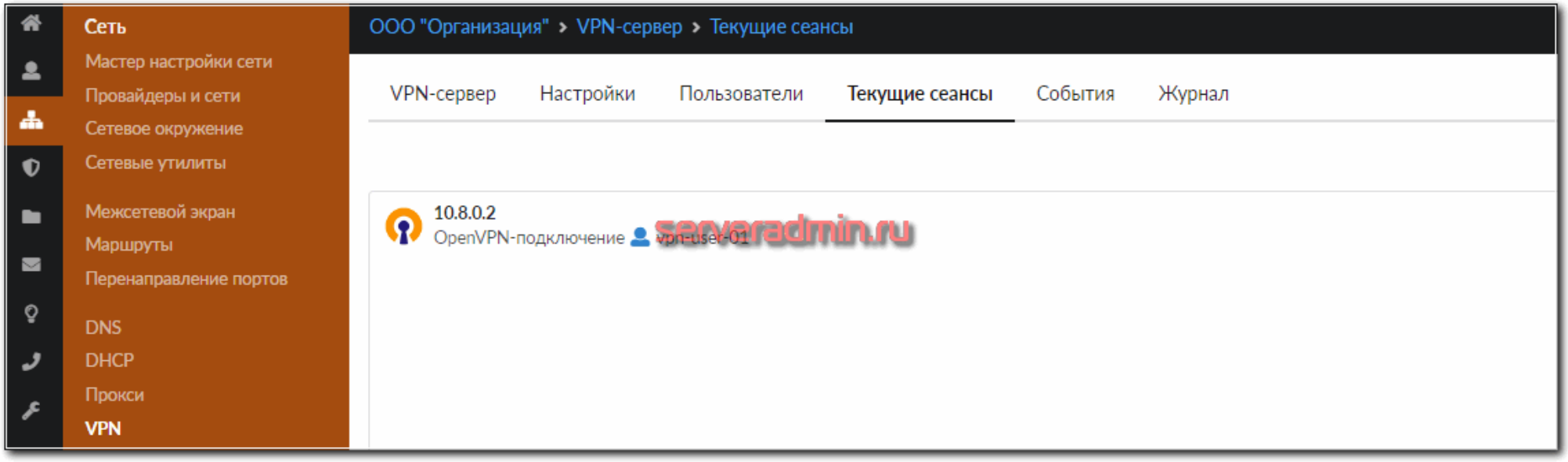
Далее идем в настройки пользователя и на вкладке OpenVPN скачиваем конфиг для подключения.


Пользователи и статистика
Пользователи
Роли
Наборы правил
Категории трафика
Монитор соединений
Диапазоны адресов
Отчеты
Управление отчетами
Сервер авторизации (Xauth)
Настройки авторизации
Captive Portal
Синхронизация
ООО "Организация" › Пользователи › vpn-user-01 › OpenVPN
Администратор
100
Состояние
Сводный отчет
IP/MAC-адреса
Правила и ограничения
Почта и телефония
Перен
OpenVPN-доступ для пользователя включен в OpenVPN-сеть (10.8.0.0/24)
Передать клиенту маршрут по умолчанию
IP клиента (опционально)
Передать клиентам маршруты до сетей
Передать клиентам маршруты до сетей
Удаленные сети за клиентом
Удаленные сети за клиентом
Сертификат клиента *
serveradmin.ru
OpenVPN-сеть_vpn-user-01
Сохранить
Обновить
Выгрузить сертификаты

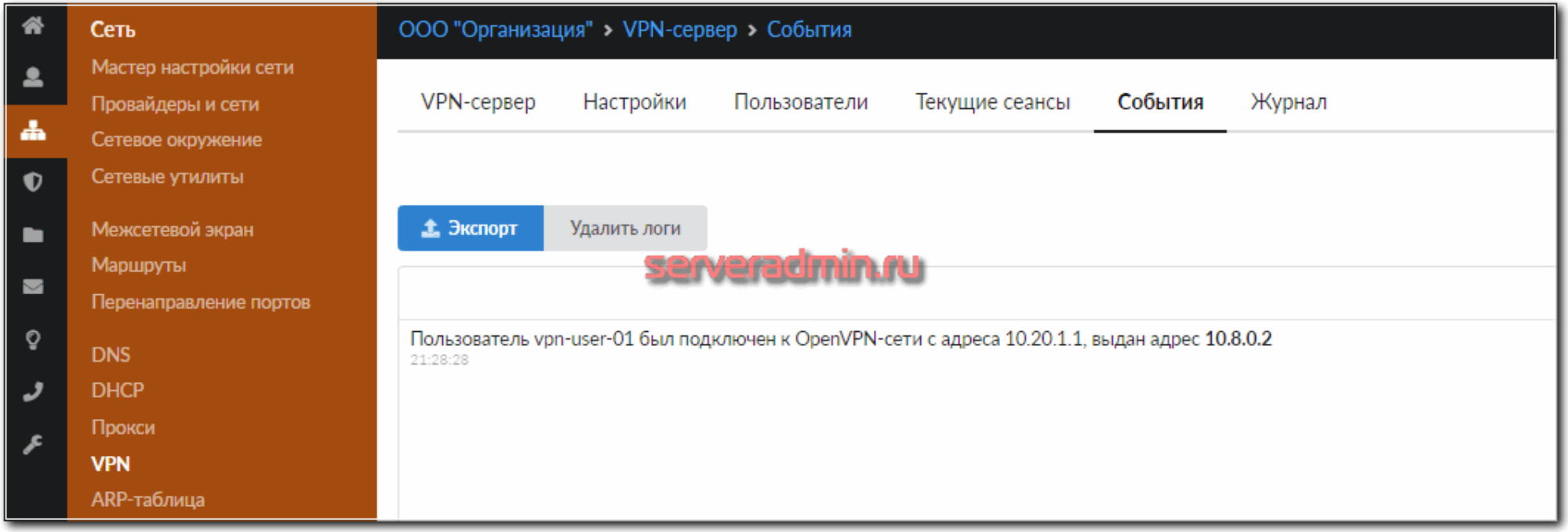
Перед выгрузкой вас попросят указать внешний интерфейс, по которому пользователи будут подключаться к openvpn серверу. Он будет указан в параметре **remote** конфига openvpn. Скачанный конфиг кладем в папку с OpenVPN и подключаемся.



Ваше подключение будет отображаться во вкладке *Текущие сеансы*.



Так же факт подключения будет записан в журнал событий.



Это удобно, когда пользователей много и нужен контроль.

Вот в целом и все. Надеюсь у вас появилось представление о том, как все это работает в интернет шлюзе ИКС. По мне так все удобно и наглядно. Можно управлять большим количеством пользователей и сетей. То есть продукт может быть одинаково полезен как для больших организаций, так и для небольших коллективов или одиночных пользователей.

К примеру, вы можете установить себе собственный шлюз на базе ИКС, завести на него несколько удаленных подсетей через openvpn client на той стороне. Раскидать маршруты по удаленным сетям и самому подключаться к этому серверу для того, чтобы получать удаленный доступ ко всем подключенным объектам. Я примерно по такой схеме давно настроил себе vpn сервер и использую для управлением своим личным хозяйством, которого у меня много.

Заключение

Как я уже сказал ранее, интернет шлюз ИКС лично мне нравится. Приятный и законченный продукт, которым можно пользоваться, если у вас есть потребность в его функционале. При этом все полностью настраивается через web интерфейс и работает. Лазить в консоль не надо вообще. То есть это история не только для линуксоидов. Даже если вы не админ, но хотите себе в офис что-то подобное, можете осилить самостоятельно с помощью документации и метода тыка.

Мне кажется такая штука хорошо зайдет для бюджетников. Например, в школы, больницы, поликлиники. Там зачастую не нужно какого-то особенного функционала, но при этом надо прикрыться документами и обеспечить соблюдение блокировки доступа по спискам гос. структур. Тут все это есть, плюс сам по себе он работает хорошо. То есть это не компромисс, когда надо соблюсти определенные требования, а потом мучиться, используя откровенно некачественный продукт, как часто бывает. ИКС приятен и удобен в использовании.