

ООО "Организация" > Сертификаты

Добавить Удалить Просмотр сертификата Импорт Экспорт

Название	Тип сертификата	Закрытый ключ	Создан	Действует до	Имя или адрес хоста
Сертификаты					
openvpn-ca	CA	не зашифрован	10.07.2020	10.07.2021	test.ru
openvpn-srv	Конечный сертификат	не зашифрован	10.07.2020	10.07.2021	test.ru
Autogenerated Asterisk_5f031654916131.49209122	Конечный сертификат	не зашифрован	06.07.2020	06.07.2030	ics-asterisk
Autogenerated GUI_5f031653cce444.37622349	Конечный сертификат	не зашифрован	06.07.2020	06.07.2030	ics-gui
Autogenerated MailServer_5f03165404e760.73013232	Конечный сертификат	не зашифрован	06.07.2020	06.07.2030	ics-mail-server

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

Что нового в ИКС 7.1

Подключение к стороннему IPSEC туннелю

Настройка своего VPN сервера

Заключение

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 подделка 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 rfsense, 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.

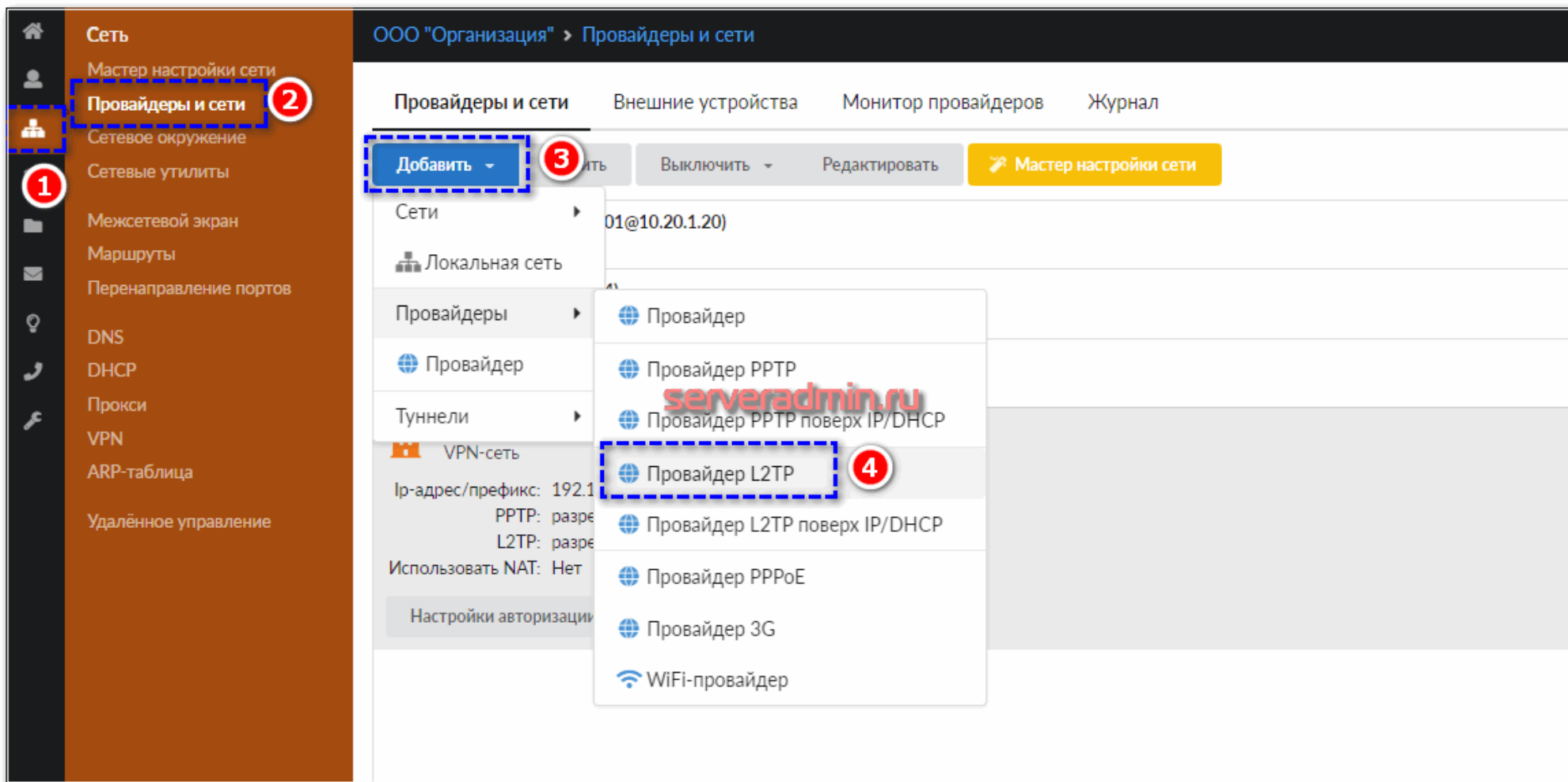
Подключение к стороннему IPSEC туннелю

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 новые подключения 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* VPN-сервер*

Логин* Пароль*

DNS

Корневые DNS Предпочитаемый DNS-сервер Альтернативный DNS-сервер

serveradmin.ru

Приоритет Ширина канала Мбит/с

Разрешить управление ИКС через веб Разрешить управление ИКС через SSH

MTU

Сохранение UDP порта

Если настроен ipsec, указываем его пароль на соседней вкладке.

Редактирование провайдера L2TP

Общие настройки **Настройки шифрования**

Использовать шифрование IPsec

Ключ *

Использовать шифрование MPPE

Ключ: (любой) Режим: (любой)

CHAP MS-CHAP MS-CHAP v2

Использовать сжатие данных

Сохранить Отмена

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

The screenshot shows the Mikrotik WinBox interface for configuring PPP. The main window displays a table with columns: Name, Type, Actual MTU, L2 MTU, Tx, Rx, Tx Packet (p/s), Rx Packet (p/s), FP Tx, FP Rx. The entry for l2tp-in1 shows L2TP Server Binding, 1450 Actual MTU, and 672 bps Tx/Rx. A 'Log' window is open in the foreground, showing a list of system messages including L2TP authentication and IPsec SA establishment.

Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx
R l2tp-in1	L2TP Server Binding	1450		672 bps	672 bps	1	1		0 bps

#	Time	Buffer	Topics	Message
29	Jul/10/2020 19:18:16	memory	l2tp, info	first L2TP UDP packet received from 10.20.1.32
30	Jul/10/2020 19:18:16	memory	l2tp, ppp, info, account	remote01 logged in, 10.40.50.99
31	Jul/10/2020 19:18:16	memory	l2tp, ppp, info	l2tp-in1: authenticated
32	Jul/10/2020 19:18:16	memory	l2tp, ppp, info	l2tp-in1: connected
33	Jul/10/2020 19:18:29	memory	ipsec, info	respond new phase 1 (Identity Protection): 10.20.1.20[500]<=>10.20.1....
34	Jul/10/2020 19:18:29	memory	ipsec, info	ISAKMP-SA established 10.20.1.20[500]-10.20.1.32[500] spi:b69cb882...
35	Jul/10/2020 19:21:04	memory	ipsec, info	purging ISAKMP-SA 10.20.1.20[500]<=>10.20.1.32[500] spi=b69cb882...
36	Jul/10/2020 19:21:04	memory	ipsec, info	ISAKMP-SA deleted 10.20.1.20[500]-10.20.1.32[500] spi:b69cb882970...
37	Jul/10/2020 19:21:04	memory	ipsec, info	respond new phase 1 (Identity Protection): 10.20.1.20[500]<=>10.20.1....
38	Jul/10/2020 19:21:04	memory	ipsec, info	ISAKMP-SA established 10.20.1.20[500]-10.20.1.32[500] spi:7cdc0709...

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 *

Ip-адрес/префикс *

Протоколы

- PPTP
- L2TP
 - L2TP IPsec

Ключ *

Использовать DPD (dead peer detection)

PPPoE

Интерфейс *

Имя сервиса

Использовать NAT

Разрешить управление ИКС через веб

Разрешить управление ИКС через SSH

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

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.

ООО "Организация" > Сетевые утилиты

Пинг Трейс Опрос Dns Информация о домене Дамп Сетевые интерфейсы

Адрес* Количество пакетов*

192.168.88.1 3

▶ Запустить

serveradmin.ru

```
PING 192.168.88.1 (192.168.88.1): 56 data bytes
64 bytes from 192.168.88.1: icmp_seq=0 ttl=64 time=0.670 ms
64 bytes from 192.168.88.1: icmp_seq=1 ttl=64 time=0.683 ms
64 bytes from 192.168.88.1: icmp_seq=2 ttl=64 time=0.668 ms

--- 192.168.88.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.668/0.674/0.683/0.007 ms
```

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)

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.

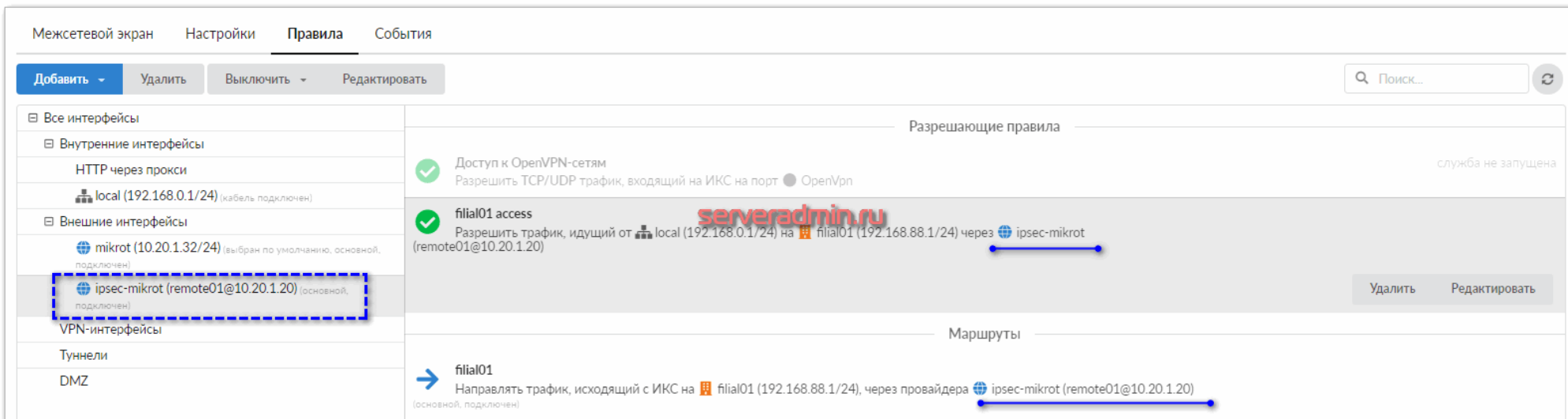
Межсетевой экран Настройки **Правила** События

Добавить Удалить Выключить Редактировать Поиск... ↻

Интерфейсы	Правило	Статус
Все интерфейсы	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
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 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	
	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)	
	Запрещающие правила	
	Запрещающее правило	

Удалить Редактировать

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.

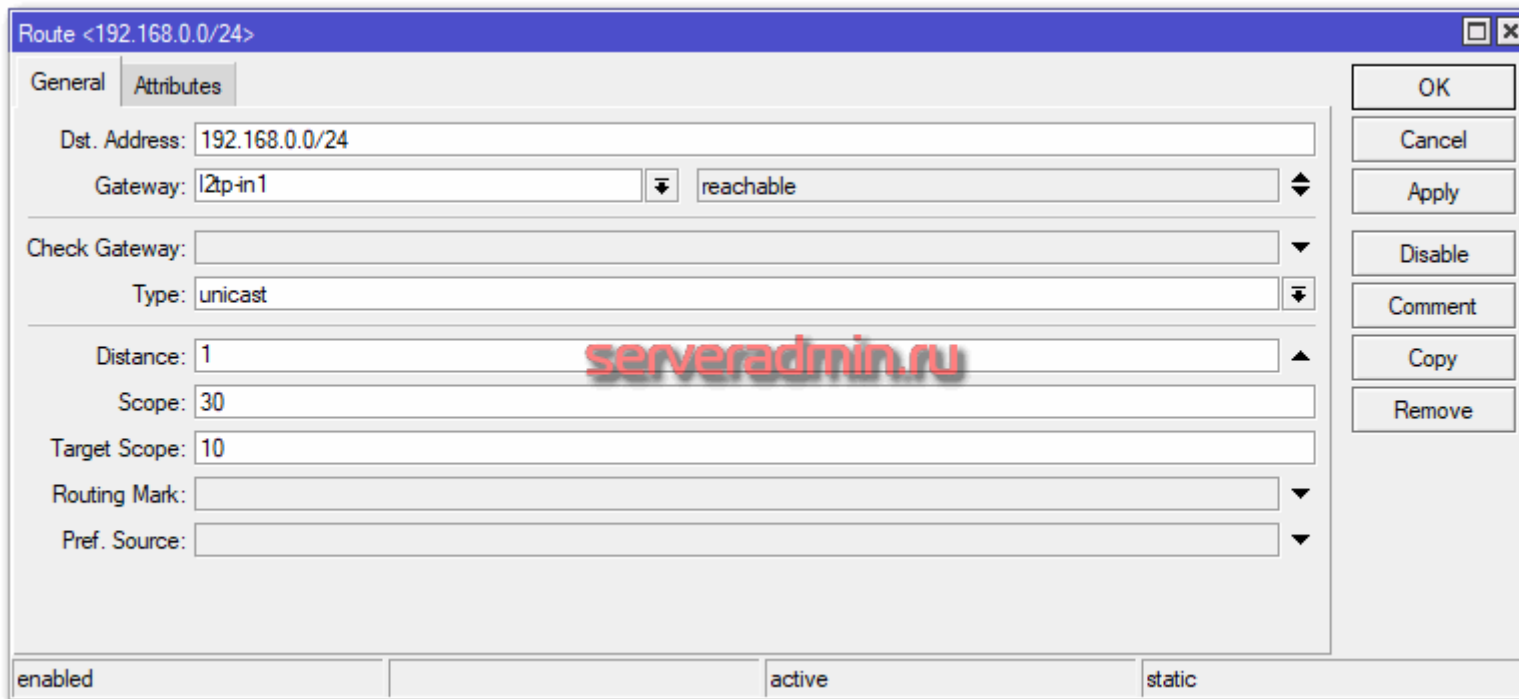


The screenshot shows the Mikrotik WinBox interface for configuring firewall rules. The 'Rules' tab is active, displaying a list of rules and their associated interfaces. The 'ipsec-mikrot (remote01@10.20.1.20)' interface is highlighted with a blue dashed box. The 'Разрешающие правила' (Allowing rules) section shows two rules: 'Доступ к OpenVPN-сетям' (Access to OpenVPN networks) and 'filial01 access'. The 'Маршруты' (Routes) section shows a route for 'filial01'.

Интерфейсы	Правило	Статус
Все интерфейсы	Разрешающие правила	
Внутренние интерфейсы		
HTTP через прокси	Доступ к OpenVPN-сетям	сервис не запущен
local (192.168.0.1/24) (кабель подключен)	Разрешить TCP/UDP трафик, входящий на ИКС на порт OpenVpn	
Внешние интерфейсы		
mikrot (10.20.1.32/24) (выбран по умолчанию, основной, подключен)	filial01 access	
ipsec-mikrot (remote01@10.20.1.20) (основной, подключен)	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)	
VPN-интерфейсы		
Туннели	Маршруты	
DMZ	filial01	
	Направлять трафик, исходящий с ИКС на filial01 (192.168.88.1/24), через провайдера ipsec-mikrot (remote01@10.20.1.20)	

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.

Сеть

Мастер настройки сети

1 Провайдеры и сети

Новое окружение

Сетевые утилиты

Межсетевой экран

Маршруты

Перенаправление портов

DNS

DHCP

Прокси

2 VPN

ARP-таблица

Удалённое управление

ООО "Организация" > VPN-сервер

Администратор 76

VPN-сервер Настройки Пользователи Текущие сеансы События Журнал

Служба PPP-соединений **запущен**

Предоставляет удаленный доступ и обеспечивает подключение PPP-провайдеров

Включить

OpenVPN **выключен**

Отвечает за работу OpenVPN-соединений

3 Включить

Журнал

[L2TP1B] IPCP: LayerUp
19:18:16

[L2TP1B] 10.40.50.99 -> 10.40.50.100
19:18:16

[L2TP1B] IFACE: Up event
19:18:16

[L2TP1B] IFACE: Rename interface ng0 to l2tp1
19:18:16

serveradmin.ru

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 *

Код страны *

Город Область

Организация E-mail

Имя или адрес хоста *

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

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.

ООО "Организация" > Сертификаты

Добавить Удалить Просмотр сертификата Импорт Экспорт

Название	Тип сертификата	Закрытый ключ
Сертификаты		
Autogenerated Asterisk_5f031654916131.49209122	Конечный сертификат	не зашифрован
Autogenerated GUI_5f031653cce444.37622349	Конечный сертификат	не зашифрован
Autogenerated MailServer_5f03165404e760.73013232	Конечный сертификат	не зашифрован
openvpn-ca	CA	не зашифрован

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.

Добавление сертификата

Общее Настройки Использование ключа Netscape расширение

Название *
openvpn-srv

Код страны *
RU - Russian Federation **serveradmin.ru**

Город Область
Город Область

Организация E-mail
Организация E-mail

Имя или адрес хоста *
test.ru

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

Добавление сертификата

Общее **Настройки** Использование ключа Netscape расширение

Тип сертификата
Конечный сертификат

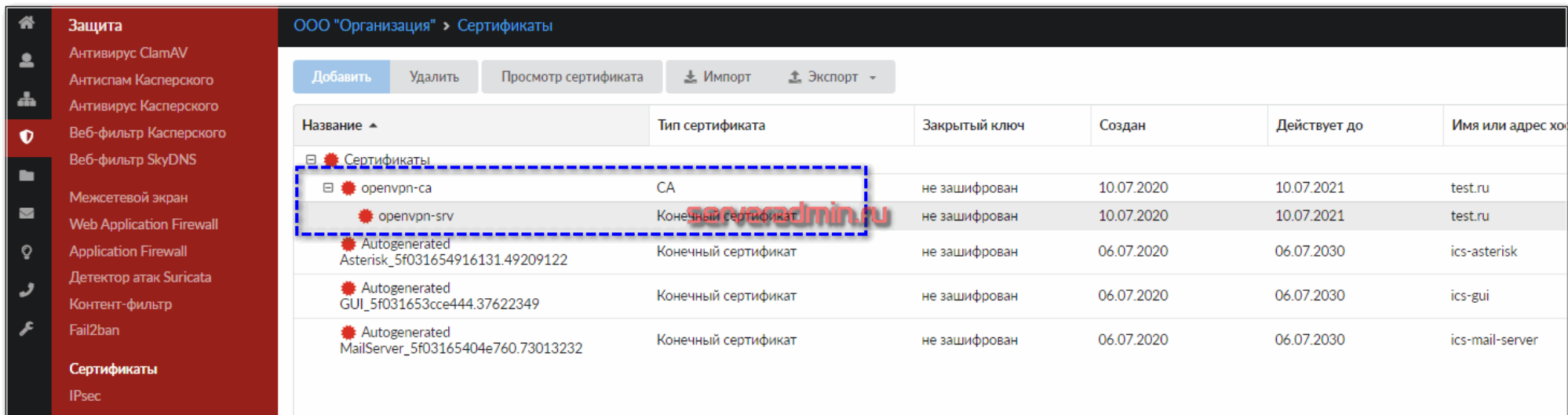
Добавить в доверенные сертификаты

Алгоритм: SHA 256 Тип шифрования: RSA

Срок действия сертификата: 10.07.2021

Длина ключа *
2048 бит

Должно получиться вот так - один сертификат за другим.



ООО "Организация" > Сертификаты

Добавить Удалить Просмотр сертификата Импорт Экспорт

Название	Тип сертификата	Закрытый ключ	Создан	Действует до	Имя или адрес хоста
Сертификаты					
openvpn-ca	CA	не зашифрован	10.07.2020	10.07.2021	test.ru
openvpn-srv	Конечный сертификат	не зашифрован	10.07.2020	10.07.2021	test.ru
Autogenerated Asterisk_5f031654916131.49209122	Конечный сертификат	не зашифрован	06.07.2020	06.07.2030	ics-asterisk
Autogenerated GUI_5f031653cce444.37622349	Конечный сертификат	не зашифрован	06.07.2020	06.07.2030	ics-gui
Autogenerated MailServer_5f03165404e760.73013232	Конечный сертификат	не зашифрован	06.07.2020	06.07.2030	ics-mail-server

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

Добавление OpenVPN-сети

Основные настройки Шифрование и сертификаты

Название *	Ир-адрес/Префикс *
<input type="text" value="OpenVPN-сеть"/>	<input type="text" value="10.8.0.0/24"/>
Протокол	Порт сервера *
<input type="text" value="UDP"/>	<input type="text" value="1194"/>

Использовать NAT

Разрешить трафик между клиентами

Передать клиенту маршрут по умолчанию

Передать клиентам маршруты до сетей

Передать клиентам DNS сервера

Разрешить управление ИКС через веб

Разрешить управление ИКС через SSH

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.

Основные настройки **Шифрование и сертификаты**

Алгоритм шифрования: AES-256-CBC

Алгоритм хеширования: SHA256


Включить сжатие LZO

Включить TLS Auth

link-MTU *: 1500

Корневой сертификат *: openvpn-ca

Сертификат сервера *: openvpn-srv



Возвращаемся в раздел VPN и добавляем пользователя.

Добавление пользователя

Общее Информация

Имя * Описание

Роль

Логин Пароль

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

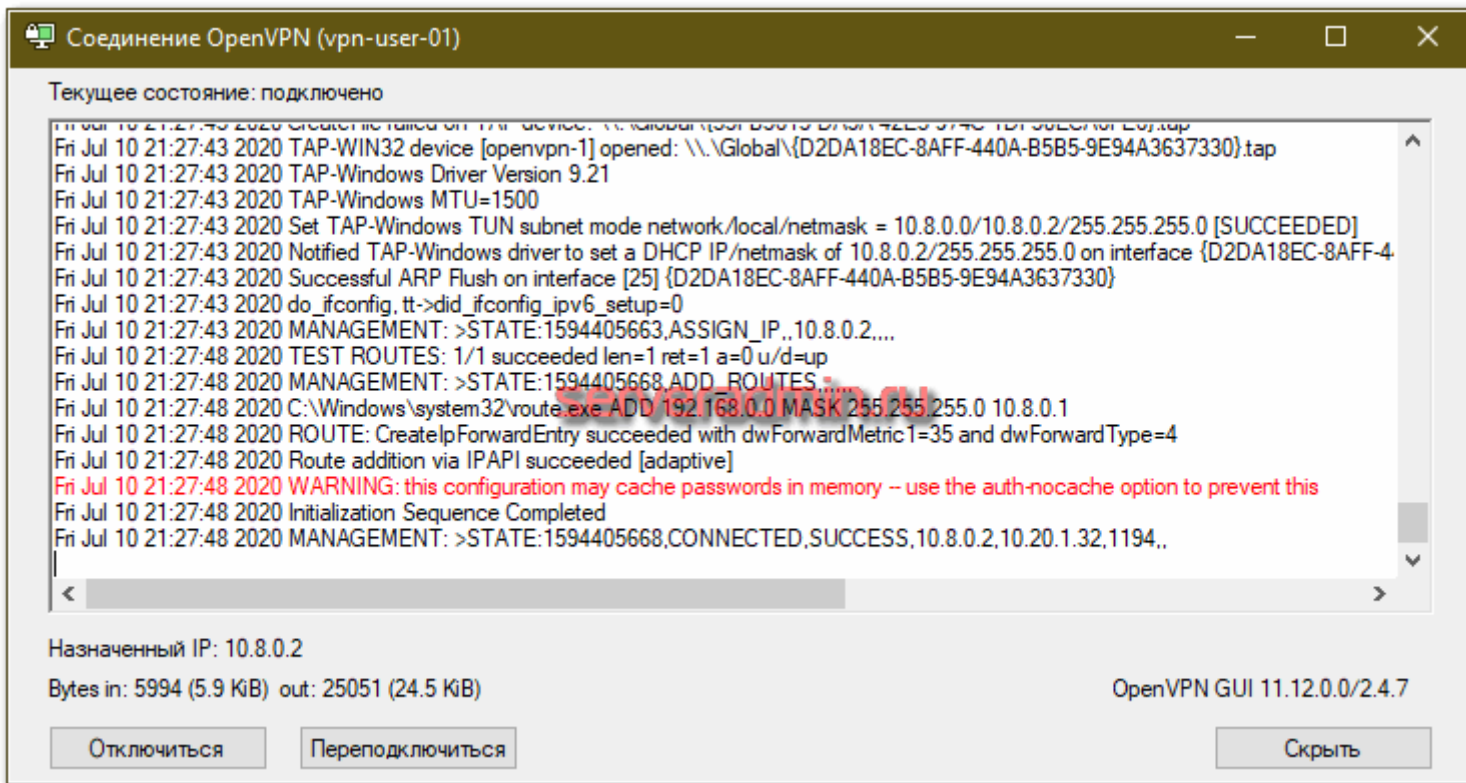
Screenshot of the Mikrotik WinBox interface showing the configuration page for VPN users. The breadcrumb path is "ООО 'Организация' > VPN-сервер > Пользователи". The user "vpn-user-01" is selected, and the "OpenVPN-доступ" checkbox is checked, indicating that the OpenVPN configuration is being downloaded for this user.

Имя	Логин	Ip-адреса из Vpn-сетей	Vpn-доступ	OpenVPN-доступ
Корневая группа			<input type="checkbox"/>	<input type="checkbox"/>
vpn-user-01	vpn-user-01		<input type="checkbox"/>	<input checked="" type="checkbox"/>
Администратор	root		<input type="checkbox"/>	<input type="checkbox"/>

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

The screenshot displays the Mikrotik WinBox interface for configuring a VPN user. The breadcrumb path is: ООО "Организация" > Пользователи > vpn-user-01 > OpenVPN. The user is currently logged in as 'Администратор'. The main configuration area shows that OpenVPN access is enabled for the user in the 'OpenVPN-сеть (10.8.0.0/24)'. There are several configuration options: a checkbox for 'Передать клиенту маршрут по умолчанию' (unchecked), a text field for 'IP клиента (опционально)', dropdown menus for 'Передать клиентам маршруты до сетей' (set to 'Передать клиентам маршруты до сетей') and 'Удаленные сети за клиентом' (set to 'Удаленные сети за клиентом'), and a certificate selection dropdown for 'Сертификат клиента *' (set to 'OpenVPN-сеть_vpn-user-01'). A red arrow points to the 'Сохранить' (Save) button at the bottom of the configuration area. The left sidebar contains navigation options like 'Пользователи и статистика', 'Роли', 'Наборы правил', etc.

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.

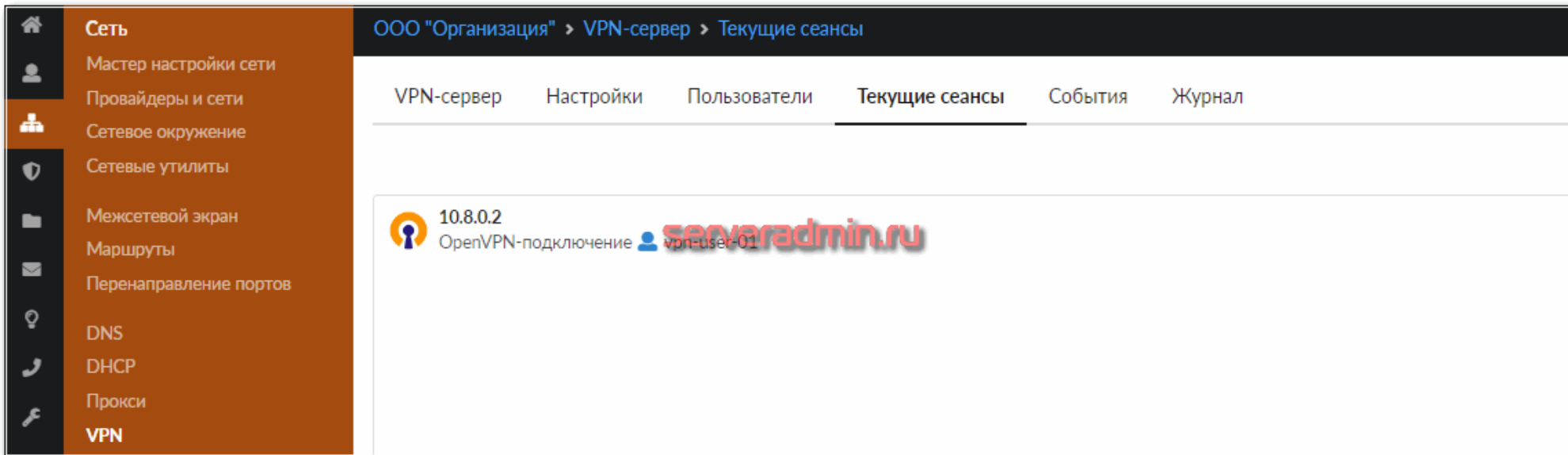


```
Текущее состояние: подключено
Fri Jul 10 21:27:43 2020 OpenVPN installed on this device: \\.\Global\{D2DA18EC-8AFF-440A-B5B5-9E94A3637330}.tap
Fri Jul 10 21:27:43 2020 TAP-WIN32 device [openvpn-1] opened: \\.\Global\{D2DA18EC-8AFF-440A-B5B5-9E94A3637330}.tap
Fri Jul 10 21:27:43 2020 TAP-Windows Driver Version 9.21
Fri Jul 10 21:27:43 2020 TAP-Windows MTU=1500
Fri Jul 10 21:27:43 2020 Set TAP-Windows TUN subnet mode network/local/netmask = 10.8.0.0/10.8.0.2/255.255.255.0 [SUCCEEDED]
Fri Jul 10 21:27:43 2020 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.8.0.2/255.255.255.0 on interface {D2DA18EC-8AFF-4
Fri Jul 10 21:27:43 2020 Successful ARP Flush on interface [25] {D2DA18EC-8AFF-440A-B5B5-9E94A3637330}
Fri Jul 10 21:27:43 2020 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Fri Jul 10 21:27:43 2020 MANAGEMENT: >STATE:1594405663,ASSIGN_IP,,10.8.0.2,...
Fri Jul 10 21:27:48 2020 TEST ROUTES: 1/1 succeeded len=1 ret=1 a=0 u/d=up
Fri Jul 10 21:27:48 2020 MANAGEMENT: >STATE:1594405668,ADD_ROUTES,....
Fri Jul 10 21:27:48 2020 C:\Windows\system32\route.exe ADD 192.168.0.0 MASK 255.255.255.0 10.8.0.1
Fri Jul 10 21:27:48 2020 ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric=35 and dwForwardType=4
Fri Jul 10 21:27:48 2020 Route addition via IPAPI succeeded [adaptive]
Fri Jul 10 21:27:48 2020 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Fri Jul 10 21:27:48 2020 Initialization Sequence Completed
Fri Jul 10 21:27:48 2020 MANAGEMENT: >STATE:1594405668,CONNECTED,SUCCESS,10.8.0.2,10.20.1.32,1194,.
```

Назначенный IP: 10.8.0.2
Bytes in: 5994 (5.9 KiB) out: 25051 (24.5 KiB) OpenVPN GUI 11.12.0.0/2.4.7

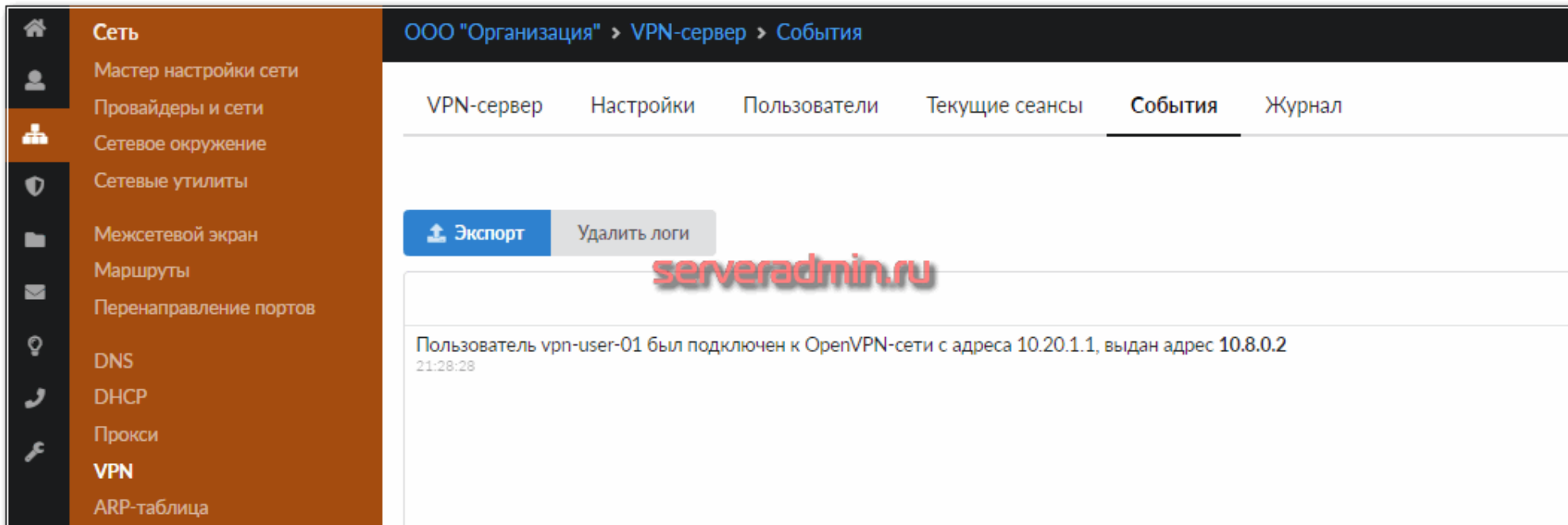
Отключиться Переподключиться Скрыть

Ваше подключение будет отображаться во вкладке *Текущие сеансы*.



Скриншот интерфейса Mikrotik WinBox, отображающий страницу «Текущие сеансы» для VPN-сервера. В левом меню выделена категория «Сеть», а в подменю — «VPN». В верхней части экрана отображены хлебные крошки: ООО "Организация" > VPN-сервер > Текущие сеансы. Над основным контентом расположены вкладки: VPN-сервер, Настройки, Пользователи, Текущие сеансы (выделена), События, Журнал. В основной области отображен один активный сеанс с IP-адресом 10.8.0.2, типом подключения OpenVPN-подключение и пользователем vpn-user-01. Водяной знак «serveradmin.ru» присутствует на изображении.

Так же факт подключения будет записан в журнал событий.



ООО "Организация" > VPN-сервер > События

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

↑ Экспорт Удалить логи

serveradmin.ru

Пользователь vpn-user-01 был подключен к OpenVPN-сети с адреса 10.20.1.1, выдан адрес 10.8.0.2
21:28:28

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.