

Настройка VPN-подключения в роутерах Mikrotik

 interface31.ru/tech_it/2019/09/nastroyka-vpn-soedineniya-v-routerah-mikrotik.html

Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Настройка VPN-подключения в роутерах Mikrotik

С ростом значения интернета в нашей повседневной жизни все более востребованными становятся различные сетевые технологии. Если раньше VPN был преимущественно уделом крупных организаций, то сегодня он используется чуть ли не в каждой сети, действительно, сотрудники стали мобильными и удаленный доступ к ресурсам сети уже не блажь, а насущная необходимость. Настройка роутера Mikrotik как VPN-клиента вопрос, на первый взгляд, простой, но есть некоторые не очевидные моменты, которые мы разберем в данной статье.



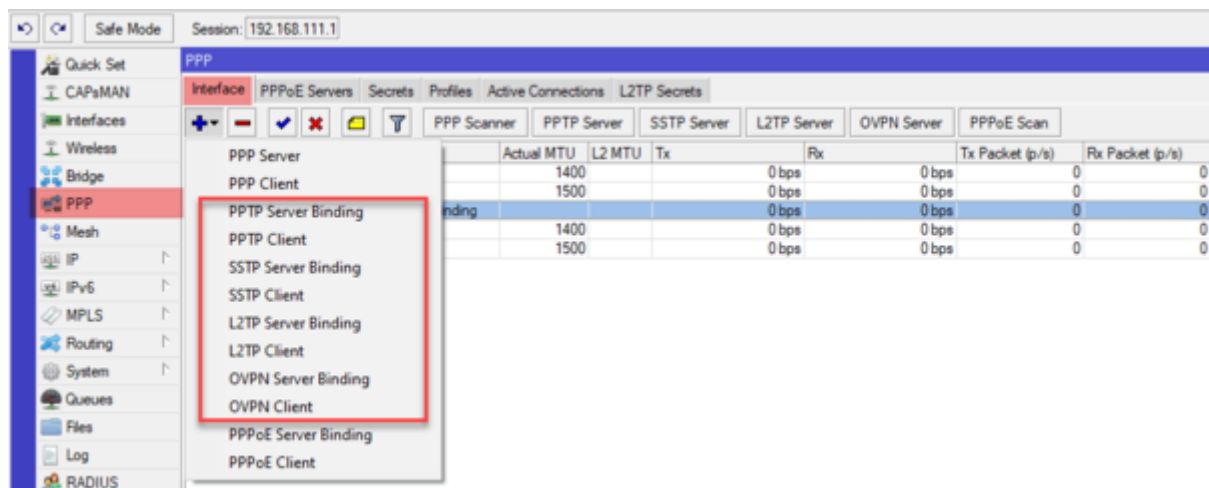
Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

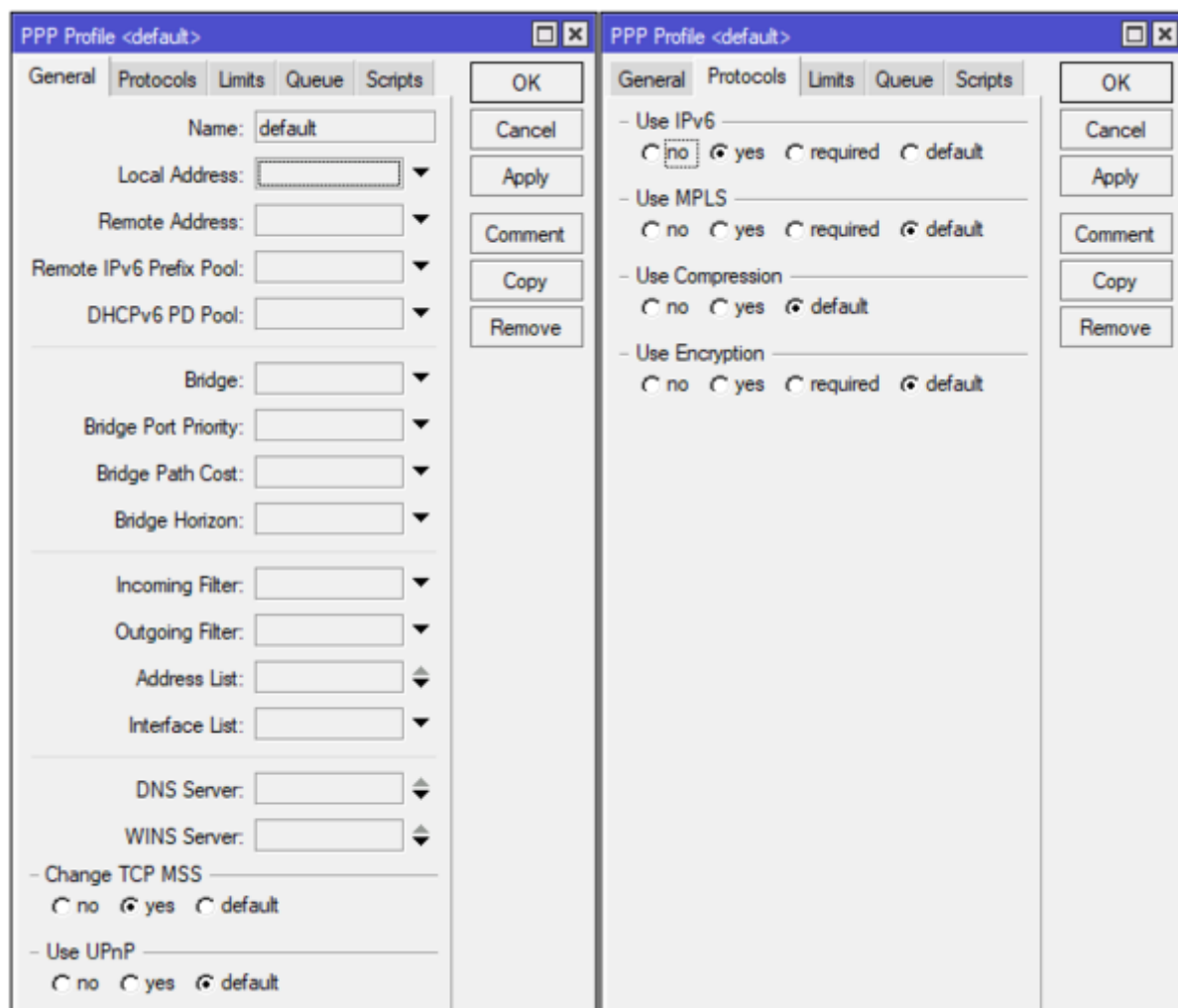
В прошлых материалах мы уже коротко рассматривали [типы VPN](#) и обращали внимание на неоднозначность используемой терминологии, традиционно термином VPN называют клиент-серверные соединения, где кроме туннельного протокола применяются вспомогательные технологии для установления соединения и контроля его состояния, аутентификации пользователя, согласования параметров подключения и т.д. и т.п. Одним из таких протоколов является PPP.

В рамках данной статьи мы будем рассматривать варианты настройки Mikrotik именно в качестве клиента для поддерживаемых типов VPN-серверов, оставив за кадром туннельные подключения (GRE, IP-IP, EoIP и т.д.). Для работы с этим типом соединений используется специальный раздел **PPP**, на закладке **Interfaces** которого можно добавить сетевой интерфейс для нужного типа VPN-клиента.

Поддерживаются PPTP, L2TP, SSTP и OpenVPN подключения. Также в списке присутствуют устаревший PPP и PPPoE, который используется для организации доступа в интернет, в данном контексте эти протоколы интереса не представляют.



Также аналогичные действия можно выполнить и в разделе Interfaces, никакой разницы откуда вы будете добавлять сетевой интерфейс нет. Но не будем спешить и перейдем на закладку **Profiles**, где находятся профили используемые при коммутируемых подключениях. По умолчанию созданы два профиля: **default** и **default-encryption**, в которых содержатся некоторые настройки для подключения. Почему некоторые? Потому что большинство опций подключения задаются сервером и клиент должен применять именно их, иначе подключение будет невозможным. Поэтому если вы заглянете в эти профили, то увидите, что большинство настроек там не активно.



Единственным различием двух профилей является опция **Use Encryption**, которая в **default-encryption** установлена в положение **yes** и требует **обязательного шифрования** подключения. Данная опция игнорируется протоколами SSTP и OpenVPN, которые **всегда** используют зашифрованные подключения.

Означает ли это, что если мы выберем профиль **default**, то ваше соединение не будет шифроваться? Нет, если сервер использует шифрование и не допускает небезопасных подключений, то ваше соединение также будет зашифровано. Но вот если сервер разрешает небезопасные подключения, то клиент вполне может подключиться без шифрования, таким образом можно осуществить атаку с подменой сервера, когда вы получите незашифрованное подключение и не будете знать об этом. Поэтому если вам явно требуется шифрование канала всегда выбирайте профиль **default-encryption**.

Мы не советуем менять настройки в стандартных профилях, если вам нужно явно задать иные настройки подключения, то создайте собственный профиль. Также учтите, что опция **Use Compression** игнорируется для OpenVPN соединений, которые в реализации от Mikrotik не могут использовать сжатие трафика.

PPTP-клиент

Пожалуй, это самый простой в настройке тип соединений. Несмотря на то, что используемое в PPTP шифрование не является надежным, этот протокол продолжает широко использоваться благодаря низким накладным расходам и высокой скорости работы, например, для доступа в интернет.

Для настройки PPTP клиента добавьте интерфейс типа **PPTP Client** и перейдите на закладку **Dial Out**, где расположены сетевые настройки.

The screenshot shows the 'New Interface' dialog box with the 'Dial Out' tab selected. The configuration fields are as follows:

- Connect To:** srv-01.lan.lab
- User:** vpnuser1
- Password:** (masked with asterisks)
- Profile:** default-encryption
- Keepalive Timeout:** 60
- ☐ Dial On Demand
- ☐ Add Default Route
- Default Route Distance:** 1
- Allow:** ☒ mschap2, ☐ mschap1, ☐ chap, ☐ pap

On the right side of the dialog, there are buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, and Torch.

Настроек немного, и они просты. В поле **Connect To** укажите FQDN или IP-адрес VPN-сервера, в поля **User** и **Password** - имя пользователя и пароль. В **Profile** выбирается в зависимости от необходимости шифрования нужный профиль. В самом низу рядом с опцией **Allow** (*разрешить*) указаны допустимые к использованию протоколы аутентификации, на сегодня безопасным считается только **MS-CHAP v2** и следует использовать по возможности только его. Однако помните, что используемый протокол аутентификации должен поддерживаться сервером, в противном случае установить связь вы не сможете.

Опция **Keepalive Timeout** указывает время переподключения соединения в случае обрыва связи. Бытует мнение, что лучше делать это значение поменьше, мол быстрее будет переподключаться туннель. Но это не так, во-первых, при неполадках на сервере вы будете активно забивать канал и нагружать сервер служебным трафиком, а во-вторых, при кратковременных перебоях связи короткое время будет вызывать переподключение с обрывом всех соединений в канале, а большее значение позволит сохранить туннель. Особенно это актуально для мобильного интернета или беспроводных каналов.

Опция **Add Default Route** создаст **маршрут по умолчанию** через туннель, т.е. направит туда весь исходящий трафик, указывайте ее только в том случае, если данный туннель **основной** способ доступа в интернет.

Никаких иных особенностей и подводных камней здесь нет и если вы правильно указали настройки, то клиент должен будет без проблем подключиться к серверу.

L2TP-клиент

Говоря про L2TP, обычно подразумевают L2TP/IPsec, потому как без шифрования данный протокол в корпоративной среде не используется. Но есть и исключения, некоторые провайдеры, например, Билайн, используют чистый L2TP без шифрования. В этом случае настройки подключения будут выглядеть так:

The image shows the 'New Interface' configuration window with the following settings:

- Connect To:** srv-01.lan.lab
- User:** uservpn1
- Password:** [masked]
- Profile:** default
- Keepalive Timeout:** 60
- Use IPsec:** ☐
- IPsec Secret:** [empty field]
- Allow Fast Path:** ☒
- Dial On Demand:** ☐
- Add Default Route:** ☒
- Default Route Distance:** 1
- Allow:**
 - ☒ mschap2
 - ☐ mschap1
 - ☐ chap
 - ☐ pap

Обратите внимание на используемый профиль - **default**, так как соединение не зашифрованное, с профилем **default-encryption** вы не сможете подключиться к серверу провайдера. **Add Default Route** ставим только если это основное соединение с интернет. Также имеет смысл использовать опцию **Allow Fast Path**, для разгрузки CPU, особенно на младших моделях, но учтите, что с данной опцией соединение может работать неустойчиво, в таком случае ее придется отключить.

Для работы с L2TP/IPsec настройки будут немного иные, во-первых, используем профиль **default-encryption** и включаем использование IPsec установкой флага **Use IPsec**, при этом становится активным поле **IPsec Secret**, куда вводим предварительный ключ.

Опция **Allow Fast Path** при использовании IPsec игнорируется и в ее установке нет никакого смысла, так же не забывайте про опцию **Add Default Route**, в большинстве корпоративных сценариев устанавливать ее не следует.

Вроде бы тоже ничего сложного в настройках L2TP/IPsec нет, но если вы попытаетесь подключиться к Windows Server, то у вас ничего не получится. В чем же дело? А дело в настройках IPsec, перейдем в **IP - IPsec - Proposal** и откроем настройку по умолчанию. **Proposal** или **предложение IPsec** содержит список алгоритмов защиты канала, которые устройство предлагает для установления соединения. Понятно, что для успешного установления канала поддерживаемые методы защиты должны совпадать.

В предложении IPsec по умолчанию обращаем внимание на опцию **PFS Group**, она отвечает за применение технологии **совершенной прямой секретности** (*Perfect forward secrecy, PFS*), которая предусматривает создание уникальных сессионных

ключей по алгоритму Диффи-Хеллмана, что делает невозможным расшифровку перехваченного IPsec трафика даже при наличии долговременных ключей (в данном случае предварительного ключа).

Windows Server по умолчанию не поддерживает совершенную прямую секретность, поэтому **PFS Group** нужно выставить в состояние **none**, после чего соединение успешно установится.

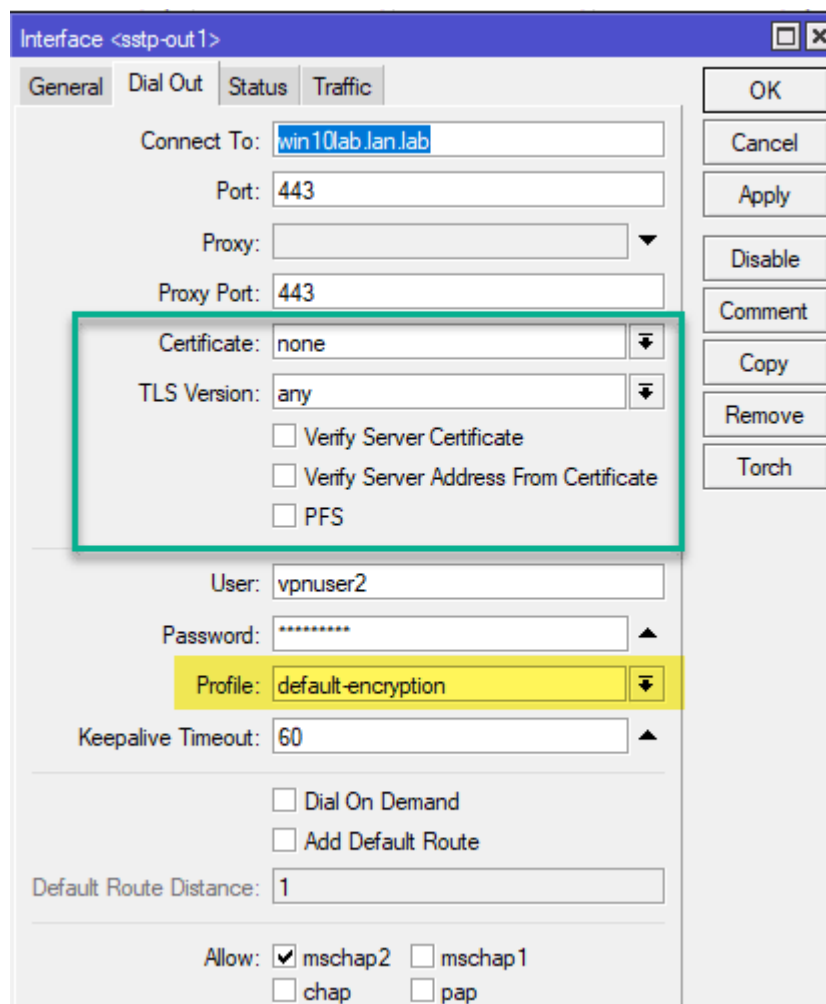
Обратите внимание, что в данном случае мы изменили настройку по умолчанию, но в данном случае это оправдано. Настройки IPsec достаточно сложны и вряд-ли человек не имеющий опыта работы с данной технологией сможет все правильно настроить с первого раза. Но это изменение следует учитывать при создании других соединений, использующих IPsec и приводить настройки с обеих сторон к общему виду.

Хотя более правильным является создание своего **предложения (Proposal)** и **политики (Policy)** для каждого соединения, но эта тема далеко выходит за рамки статьи.

SSTP-клиент

Мы не будем останавливаться на уже описанных нами опциях, которые общие для всех видов коммутируемых подключений, а сосредоточимся на новых, свойственных именно этому типу VPN. SSTP относится к отдельной подгруппе SSL VPN, которые используют трафик практически не отличимый от HTTPS, что серьезно затрудняет выявление и блокирование таких туннелей.

На что следует обратить внимание при настройке? Давайте сначала посмотрим на окно настроек:



Как видим, появилась опция **Port**, где мы можем указать порт подключения, по умолчанию это 443, но можно использовать и любой иной, если 443 порт занят, например, веб-сервером. Также SSTP может прекрасно работать через прокси, в этом случае вам потребуется указать адрес прокси-сервера и используемый им порт в опциях **Proxy** и **Proxy Port**.

Также вспоминаем, что SSTP всегда использует шифрование канала, поэтому оно будет работать вне зависимости от выбранного профиля, в данном случае **default** и **default-encryption** будут работать одинаково.

Теперь перейдем к специфичным для протокола настройкам, которые мы обвели зеленой рамкой. Поле **Certificate** используется для указания клиентского сертификата в том случае, если сервер использует аутентификацию по сертификатам, в этом случае его потребуется загрузить на устройство и импортировать в разделе **System - Certificates**. Во всех остальных случаях в поле должно стоять **none**.

TLS Version указывает на допустимые к использованию версии TLS, однако это определяется сервером, но следует стараться использовать только протокол TLS 1.2, что позволяет исключить атаки с понижением протокола.

Опция **Verify Server Certificate** не является обязательной, но позволяет проверить подлинность сервера, исключая атаки типа человек посередине, для этого потребуется импортировать на Mikrotik сертификат центра сертификации (CA) выдавшего сертификат серверу.

Опция **Verify Server Address From Certificate** позволяет убедиться, что IP-адрес подключения соответствует адресу для имени, указанного в сертификате. Также не является обязательной, но позволяет дополнительно убедиться, что подключаетесь вы именно к тому серверу.

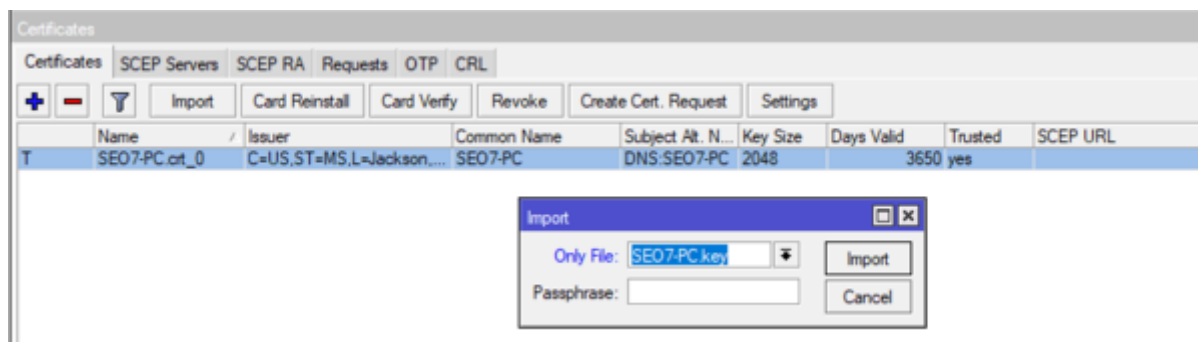
Установка флага в поле **PFS** включает **совершенную прямую секретность**, но эта опция должна поддерживаться со стороны сервера.

OpenVPN-клиент

Реализация OpenVPN в Mikrotik вызывает много нареканий, так как сводит на нет все сильные стороны данной технологии и делает ощутимыми слабые. OpenVPN-клиент не поддерживает сжатие данных и работу по протоколу UDP, если первое не столь значимо на современных каналах, то OpenVPN поверх TCP имеет очень большие накладные расходы и вызывает как повышенную нагрузку на оборудование, так и плохую утилизацию канала. Поэтому от использования OpenVPN на Mikrotik по возможности следует отказаться.

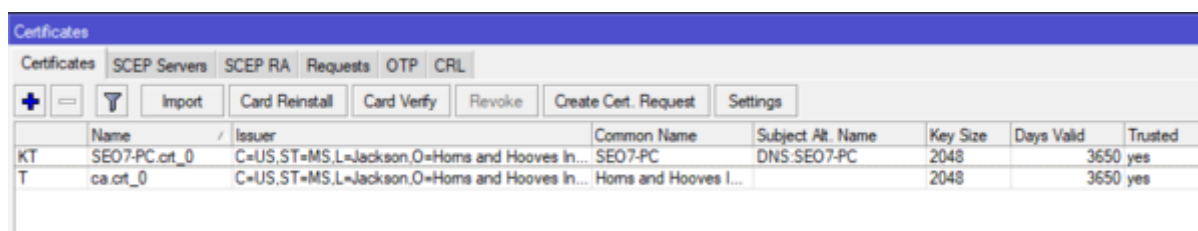
Обычно комплект для подключения OpenVPN клиента составляют сертификат CA, сертификат и закрытый ключ клиента, конфигурационный файл. Нам понадобятся только сертификат и ключ клиента, а если мы хотим проверять подлинность сервера, то еще и сертификат CA, но он не является обязательным для настройки подключения.

Прежде всего загрузим сертификаты и ключи на Mikrotik, затем перейдем в **System - Certificates** и импортируем сертификат клиента. Он появится в списке сертификатов и напротив него будет буква **T**, что обозначает **trusted**, т.е. устройство доверяет этому сертификату. Затем импортируем ключ, здесь важно соблюдать именно эту последовательность, сначала сертификат, потом ключ.



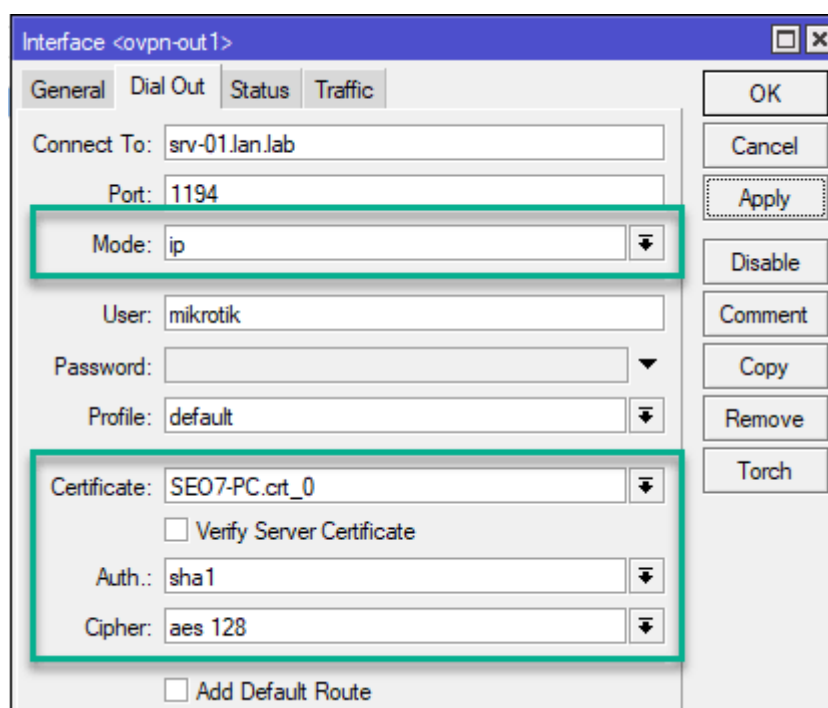
После успешного импорта ключа флаги сменятся на **КТ**, где буква К обозначает наличие закрытого ключа для сертификата. Затем аналогичным образом импортируем сертификат CA сервера, импорт ключа для данного сертификата не

нужен. Закрытый ключ СА является самой большой тайной и должен храниться с соблюдением всех мер предосторожности и не при каких обстоятельствах не должен покидать узел СА (центра сертификации).



	Name	Issuer	Common Name	Subject Alt. Name	Key Size	Days Valid	Trusted
KT	SEO7-PC.crt_0	C=US, ST=MS, L=Jackson, O=Horns and Hooves In...	SEO7-PC	DNS:SEO7-PC	2048	3650	yes
T	ca.crt_0	C=US, ST=MS, L=Jackson, O=Horns and Hooves In...	Horns and Hooves I...		2048	3650	yes

Теперь рассмотрим поближе окно настроек подключения, адрес подключения и порт не должны вызвать затруднений, а вот остальные опции нуждаются в пояснении, значимые мы выделили зеленой рамкой.



Interface <ovpn-out1>

General Dial Out Status Traffic

Connect To: srv-01.lan.lab

Port: 1194

Mode: ip

User: mikrotik

Password:

Profile: default

Certificate: SEO7-PC.crt_0

☐ Verify Server Certificate

Auth.: sha1

Cipher: aes 128

☐ Add Default Route

OK Cancel Apply Disable Comment Copy Remove Torch

Но сначала коснемся опций **User** и **Profile**. Первая используется только в случае аутентификации на сервере по имени и паролю, большинство OpenVPN серверов такой тип аутентификации не используют и в этом поле вы можете написать все что угодно, просто оно должно быть заполнено. Профиль также не имеет значения, так как OpenVPN всегда шифрует канал, а опцию сжатия игнорирует.

Mode задает режим работы канала, в терминах OpenVPN **ip** - это **tun** (L3), а **ethernet** - это **tap** (L2), следует помнить, что режим работы определяется сервером. В поле **Certificate** укажите импортированный **сертификат клиента**. Опции **Auth** и **Cipher** указывают на используемые сервером криптографические алгоритмы для аутентификации и шифрования, если вы укажете отличные от указанных в конфигурации сервера - то соединение установить не удастся. Если алгоритм аутентификации явно не указан в конфигурации сервера, то по умолчанию используется SHA1.

При настройке OpenVPN клиента на Mikrotik следует помнить, что сервер должен поддерживать соединения по протоколу TCP, без сжатия и TLS-аутентификации, в противном случае подключиться к серверу не удастся.

Опция **Verify Server Certificate** позволяет проверить подлинность сертификата сервера, что защищает от атак типа человек посередине, но требует импорта сертификата CA сервера.

Маршрутизация

Если VPN соединение используется для доступа к корпоративной сети или предназначено для связи сетей, то вам потребуется указать маршруты для правильной пересылки пакетов. Так если мы хотим получить доступ к сети за VPN-сервером, то нам потребуется создать маршрут к этой сети, указав в качестве шлюза интерфейс нашего VPN-клиента, например так:

The screenshot shows the 'Route' configuration window in Mikrotik WinBox. The title bar reads 'Route <192.168.200.0/24>'. The window has two tabs: 'General' and 'Attributes', with 'General' currently selected. The configuration fields are as follows:

- Dst. Address:** 192.168.200.0/24
- Gateway:** l2tp-out1 (selected from a dropdown menu)
- Check Gateway:** (empty dropdown menu)
- Type:** unicast (selected from a dropdown menu)
- Distance:** 1
- Scope:** 30
- Target Scope:** 10
- Routing Mark:** (empty dropdown menu)
- Pref. Source:** 192.168.111.1

On the right side of the window, there is a vertical stack of buttons: OK, Cancel, Apply, Disable, Comment, Copy, and Remove. At the bottom of the window, there are three status indicators: 'enabled', 'active', and 'static'.

В данном примере мы отправляем все пакеты к сети 192.168.200.0/24 через L2TP-подключение l2tp-out1. Если вы понимаете основы маршрутизации, то указание правильных маршрутов для вас не составит труда.

Отдельного внимания заслуживает опция **Pref. Source**, которая не является обязательной, но ее следует указывать, если роутер обслуживает несколько сетей, в ней указывается адрес, с которого роутер будет посылать пакеты по указанному маршруту. Без ее указания доступ роутера к ресурсам удаленных сетей может оказаться невозможным (как и удаленных сетей к нему), на работу клиентов в сетях это не влияет. В качестве значения следует указать адрес, принадлежащий той сети, к которой имеется маршрут с противоположной стороны (т.е. сети за сервером).

Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на углубленном курсе по администрированию MikroTik. Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.
