

Настройка PPTP или L2TP VPN-сервера на роутерах Mikrotik

 interface31.ru/tech_it/2021/01/nastroyka-pptp-ili-l2tp-vpn-server-na-routerah-mikrotik.html

Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Настройка PPTP или L2TP VPN-сервера на роутерах Mikrotik

Продолжая актуальную сегодня тему удаленного доступа, сегодня мы рассмотрим настройку роутеров Mikrotik для использования из в качестве PPTP или L2TP VPN-серверов. С одной стороны тема эта, вроде бы простая, с другой, как обычно, имеет свои особенности, которые следует учитывать еще на стадии выбора решения. Ведь хороший специалист выбирает инструмент под задачу, а не пытается делать наоборот, признавая сильные и слабые стороны каждого решения.



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.

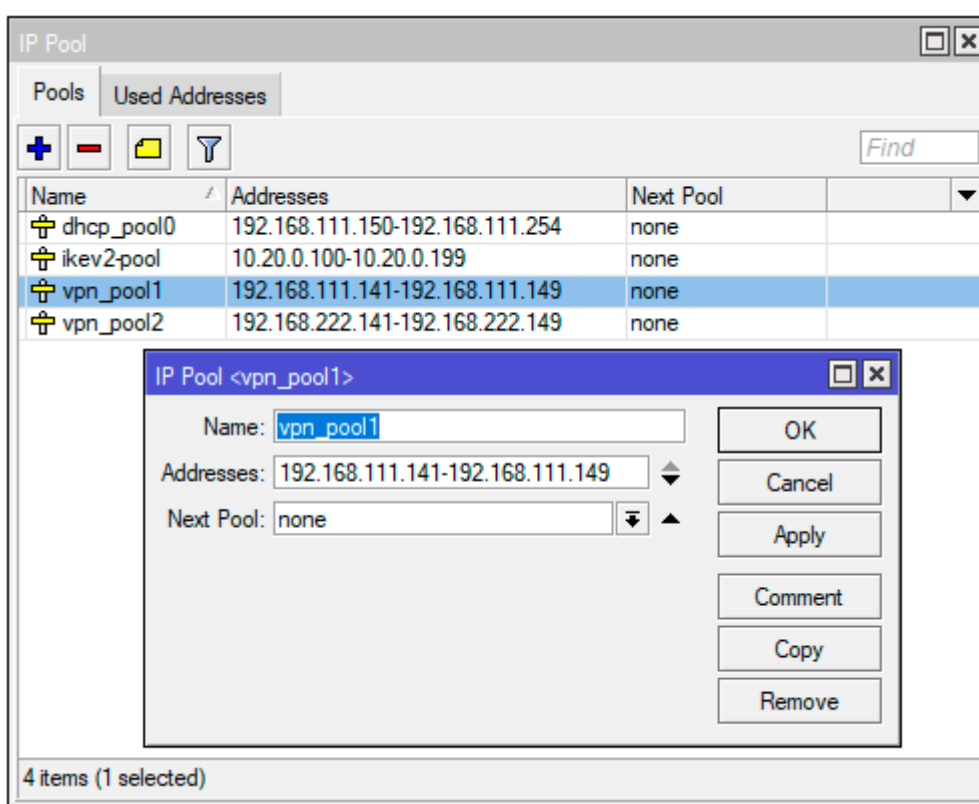
Перед тем, как браться за настройку VPN-сервера на базе Mikrotik мы рекомендуем вам ознакомиться с нашим материалом: [Производительность младших моделей Mikrotik hEX и hAP. Экспресс-тестирование](#). Если коротко: на моделях без аппаратной поддержки AES вы не получите для соединений L2TP/IPsec скоростей более 25-30 МБит/с, на моделях с поддержкой AES скорость упирается в 35-50 МБит/с. В большинстве случаев для сценария удаленного доступа этого достаточно, но все-таки данный момент обязательно следует иметь ввиду, чтобы не получить потом претензию, что Mikrotik работает плохо и этому объективно будет нечего противопоставить.

Что касается PPTP, то здесь все достаточно хорошо, даже недорогие модели роутеров позволяют достигать скоростей около 100 МБит/с, но при этом следует помнить, что PPTP имеет слабое шифрование и не считается безопасным в современных реалиях. Однако он может быть неплохим выбором, если вы хотите завернуть в него изначально защищенные сервисы, например, при помощи SSL.

Предварительная настройка роутера

Прежде чем начинать настройку VPN-сервера нужно определиться со структурой сети и выделить для удаленных клиентов пул адресов. Если брать сценарий удаленного доступа, то здесь есть два основных варианта: Proxy ARP, когда клиенты получают адреса из диапазона локальной сети и имеют доступ к ней без дополнительных настроек и вариант с маршрутизацией, когда клиентам выдаются адреса из диапазона не пересекающегося с локальной сетью, а для доступа в сеть на клиентах добавляются необходимые маршруты. В современных Windows-системах это можно автоматизировать при помощи PowerShell.

После того, как вы определились со структурой сети, следует перейти в **IP - Pool** и создать новый пул адресов для выдачи удаленным клиентам. Количество адресов в пуле должно соответствовать количеству планируемых VPN-клиентов, либо превышать его.

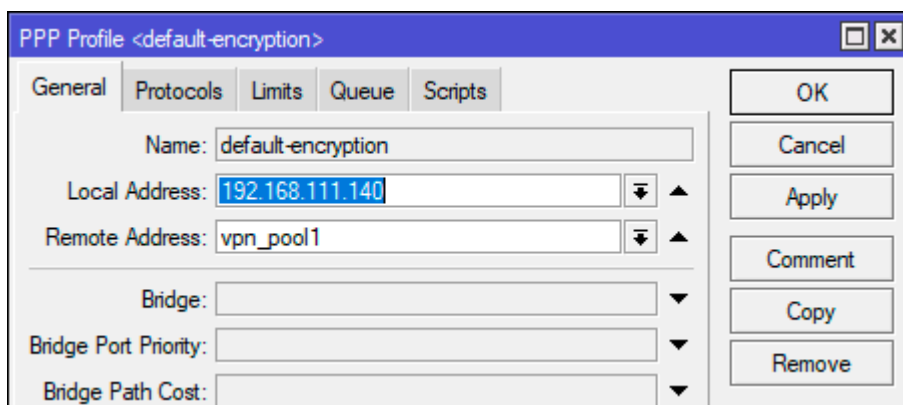


Эти же действия в терминале:

```
/ip pool  
add name=vpn_pool1 ranges=192.168.111.141-192.168.111.149
```

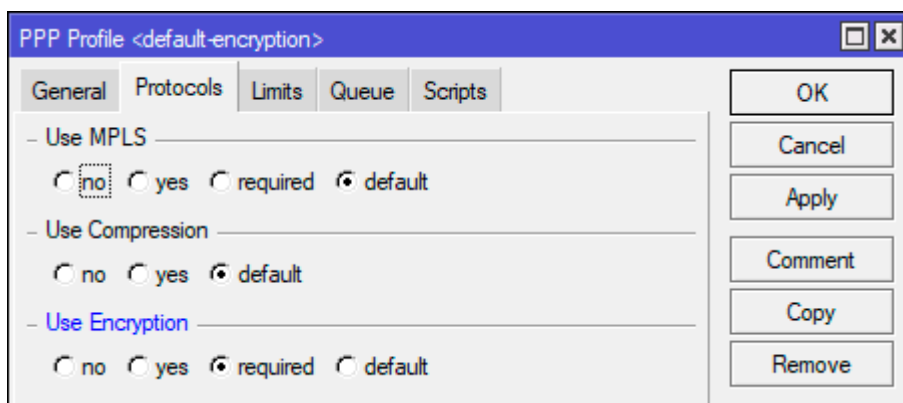
Затем перейдем в **PPP - Profiles** и настроим профиль для нашего VPN-сервера, который будет содержать базовые настройки. Если вы настраиваете сразу и PPTP и L2TP-сервера, то можете использовать для них как общий профиль, так и создать отдельные. В случае с общим профилем они будут иметь общий адрес сервера и общий пул адресов. В данном разделе уже существуют два стандартных профиля **default** и **default-encryption**, поэтому при желании можете не создавать новые профили, а настроить имеющиеся.

На вкладке **General** задаем параметры: **Local Address** - локальный адрес сервера, должен принадлежать к тому же диапазону, что и пул адресов, который вы задали выше, **Remote Address** - адреса для выдачи удаленным клиентам, указываем в этом поле созданный пул.



The screenshot shows the 'PPP Profile <default-encryption>' window with the 'General' tab selected. The 'Name' field is 'default-encryption'. The 'Local Address' field is '192.168.111.140'. The 'Remote Address' field is 'vpn_pool1'. There are also fields for 'Bridge', 'Bridge Port Priority', and 'Bridge Path Cost', all of which are currently empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

Следящая вкладка - **Protocols**, здесь мы рекомендуем установить параметр **Use Encryption** в положение **required**, что будет требовать от клиента обязательного использования шифрования.



The screenshot shows the 'PPP Profile <default-encryption>' window with the 'Protocols' tab selected. Under 'Use MPLS', the 'no' radio button is selected. Under 'Use Compression', the 'default' radio button is selected. Under 'Use Encryption', the 'required' radio button is selected. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

Чтобы добавить новый профиль в терминале выполните (в данном случае мы создаем профиль с именем **vpn**):

```
/ppp profile
add change-tcp-mss=yes local-address=192.168.111.140 name=vpn remote-
address=vpn_pool1 use-encryption=required
```

Чтобы изменить существующий **default-encryption**:

```
/ppp profile
set *FFFFFFFE local-address=192.168.111.140 remote-address=vpn_pool1 use-
encryption=required
```

Для **default** вместо **set *FFFFFFFE** укажите **set *0**:

```
/ppp profile
set *0 local-address=192.168.111.140 remote-address=vpn_pool1 use-
encryption=required
```

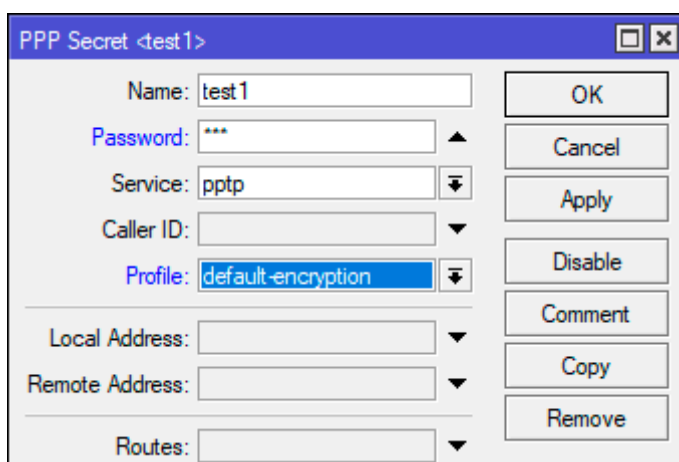
Остальные параметры оставляем без изменений, для удаленных клиентов они **не применяются** (в том числе сжатие) и работают только при соединении между устройствами с RouterOS. Отсутствие сжатия также следует учитывать, особенно если ваши клиенты используют медленные каналы подключения, скажем 3G-модемы.

Теперь добавим пользователей, для этого откроем **PPP - Secrets** и создадим новую учетную запись. Обязательно заполняем поля: **Name** и **Password**, а также **Profile**, где указываем созданный на предыдущем шаге профиль, если профили клиента и сервера не будут совпадать - подключение окажется невозможным. Поле **Service** позволяет ограничить действие учетных данных только одним сервисом, для этого нужно указать его явно, если же вы хотите использовать одни учетную запись для всех видов подключения - оставьте значение по умолчанию **any**.

В терминале:

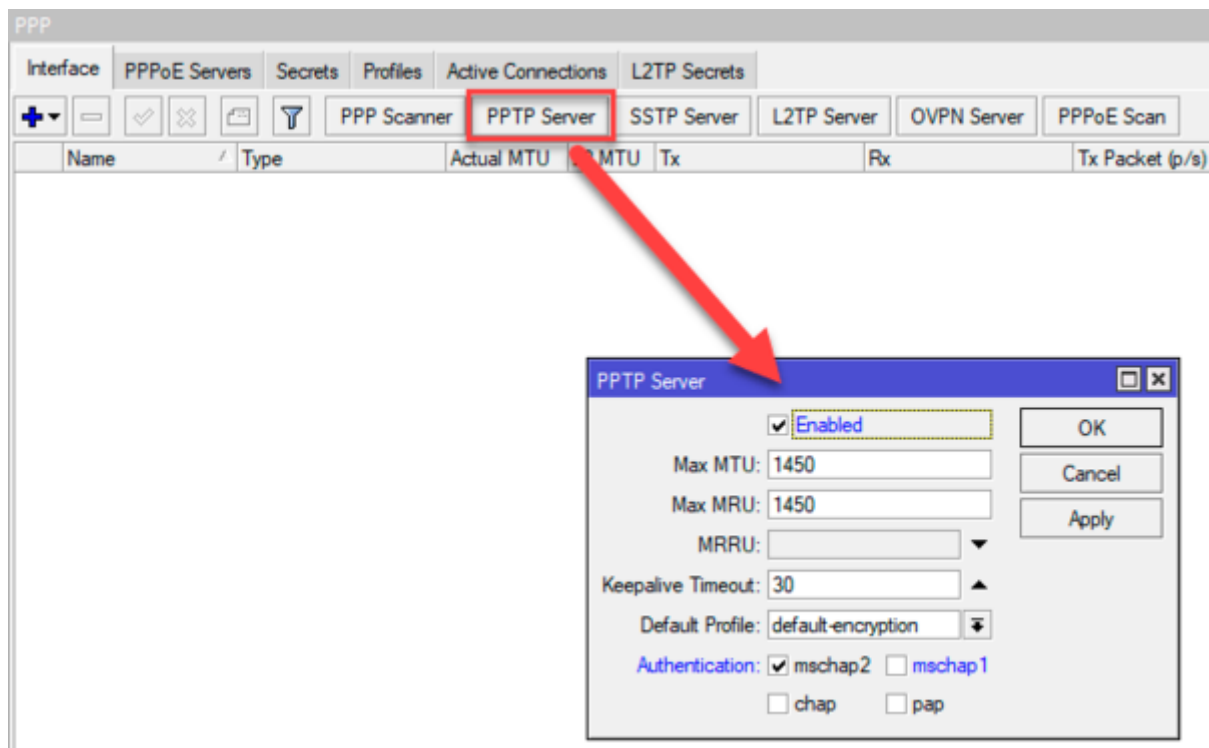
```
/ppp secret  
add name=test1 password=123  
profile=default-encryption  
service=pptp
```

При создании учетных данных уделите должное внимание политике паролей, особенно для PPTP.



Настройка PPTP-сервера

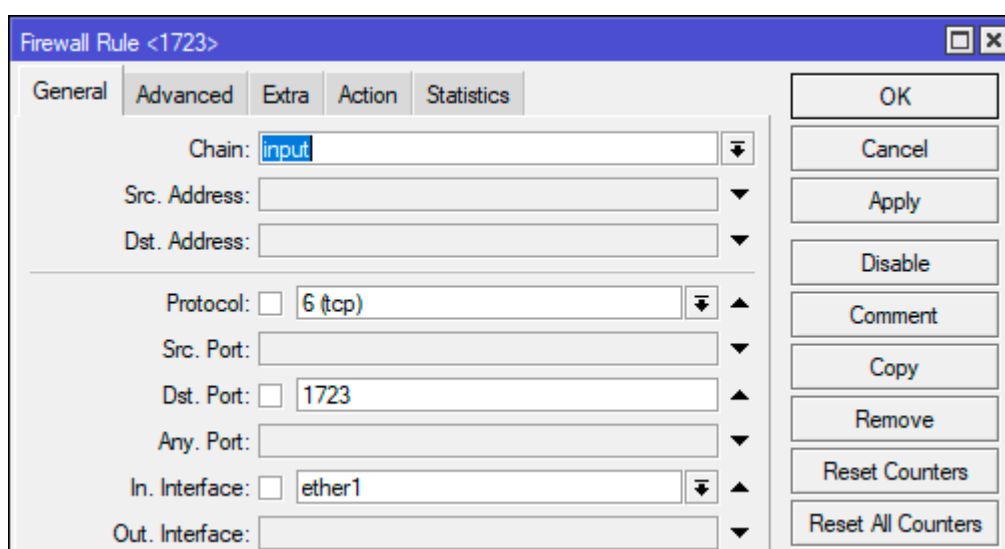
Настроить PPTP-сервер в RouterOS просто. Откройте **PPP - Interface** и нажмите кнопку **PPTP Server**, в открывшемся окне установите флаг **Enabled**, в поле **Default Profile** укажите созданный на подготовительном этапе профиль и в разделе **Authentication** оставьте только **mschap2**.



Это же действие в терминале:

```
/interface pptp-server server
set authentication=mschap2 default-profile=default-encryption enabled=yes
```

Следующим шагом следует разрешить подключения к нашему VPN-серверу в брандмауэре, для этого следует разрешить входящие подключения для порта **1723 TCP**. Открываем **IP - Firewall** и создаем новое правило: **Chain - input, Protocol - tcp, Dst. Port - 1723**, в поле **In. Interface** указываем внешний интерфейс роутера, в нашем случае ether1. Так как действие по умолчанию - **accept** то просто сохраняем правило.



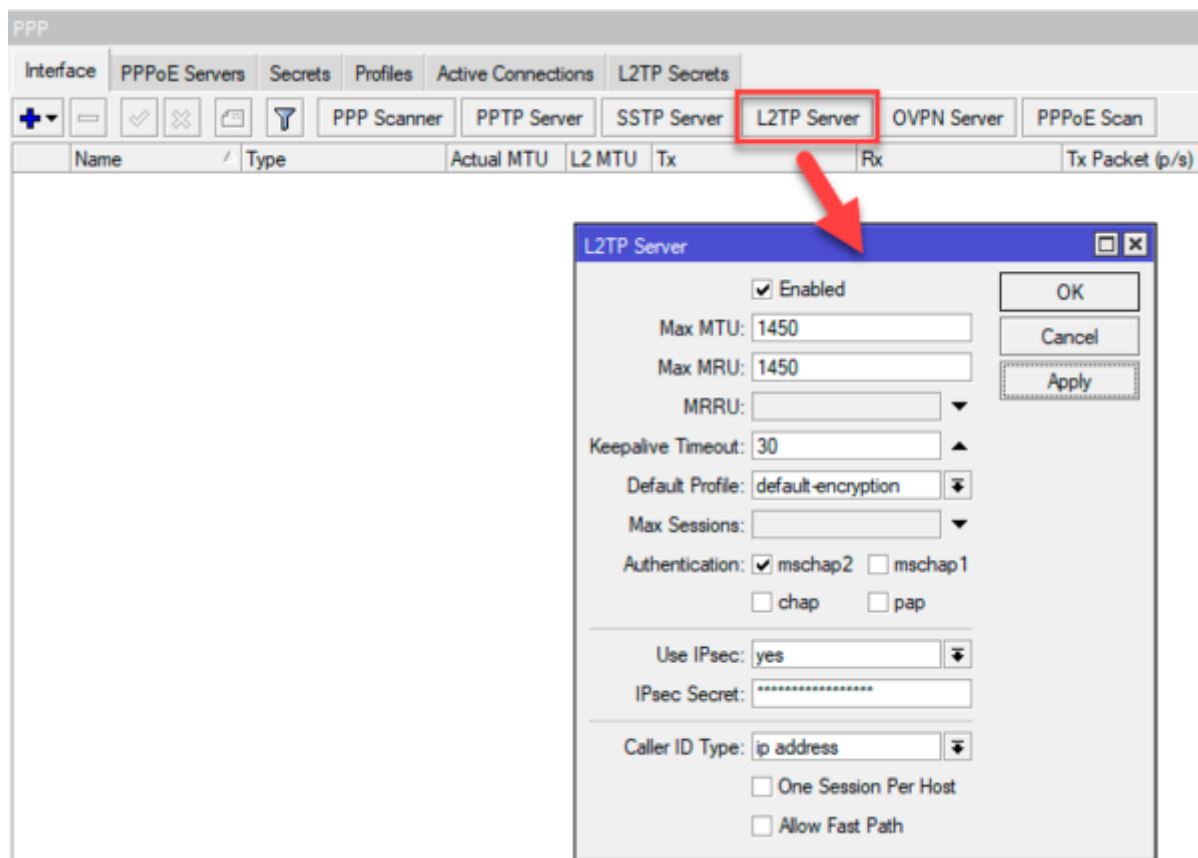
В терминале создать правило можно командой:

```
add action=accept chain=input dst-port=1723 in-interface=ether1 protocol=tcp
```

На этом настройку PPTP-сервера можно считать законченной, он готов принимать подключения.

Настройка L2TP/IPsec-сервера

Точно также, как и при настройке PPTP-сервера переходим в **PPP - Interface** и нажимаем кнопку **L2TP Server**. В открывшемся окне ставим флаг **Enabled**, в **Default Profile** указываем созданный ранее профиль, а в **Authentication** оставляем только **mschap2**. Затем включаем использование IPsec - **Use IPsec - yes** и в поле **IPsec Secret** вводим предварительный ключ соединения:



Для включения сервера с указанными настройками в терминале выполните:

```
/interface l2tp-server server
set authentication=mschap2 enabled=yes default-profile=default-encryption ipsec-
secret=myIPsecPreKey use-ipsec=yes
```

Обычно на этом инструкции по настройке L2TP-сервера заканчиваются, но если оставить все как есть, то у сервера будут достаточно слабые настройки шифрования, поэтому подтянем их до современного уровня. Для этого нам потребуется изменить параметры IPsec, так как L2TP сервер безальтернативно использует параметры по умолчанию будем менять именно их.

Переходим в **IP - IPsec - Proposal** и приводим набор настроек **default** к следующему виду: **Auth. Algorithms** - sha1, sha256, **Encr. Algorithms** - aes-128-cbc, aes-192-cbc, aes-256-cbc, **PFS Group** - ecp384.

Данные настройки в терминале:

```
/ip ipsec proposal
set [ find default=yes ] auth-
algorithms=sha256,sha1 pfs-
group=ecp384
```

Затем откроем **IP - IPsec - Profiles** и изменим настройки профиля **default**: **Encryption Algorithm - aes256, DH Group - modp2048, ecp256, ecp384**.

IPsec Proposal <default>

Name: default

Auth. Algorithms: ☐ md5 ☒ sha1
☐ null ☒ sha256
☐ sha512

Encr. Algorithms: ☐ null ☐ des
☐ 3des ☒ aes-128 cbc
☒ aes-192 cbc ☒ aes-256 cbc
☐ blowfish ☐ twofish
☐ camellia-128 ☐ camellia-192
☐ camellia-256 ☐ aes-128 ctr
☐ aes-192 ctr ☐ aes-256 ctr
☐ aes-128 gcm ☐ aes-192 gcm
☐ aes-256 gcm

Lifetime: 00:30:00 ▲

PFS Group: ecp384 ▼

enabled default

Buttons: OK, Cancel, Apply, Disable, Copy, Remove

IPsec Profile <default>

Name: default

Hash Algorithms: sha1 ▼

PRF Algorithms: auto ▼

Encryption Algorithm: ☐ des ☐ 3des
☐ aes-128 ☐ aes-192
☒ aes-256 ☐ blowfish
☐ camellia-128 ☐ camellia-192
☐ camellia-256

DH Group: ☐ modp768 ☐ modp1024
☐ ec2n155 ☐ ec2n185
☐ modp1536 ☒ modp2048
☐ modp3072 ☐ modp4096
☐ modp6144 ☐ modp8192
☒ ecp256 ☒ ecp384
☐ ecp521

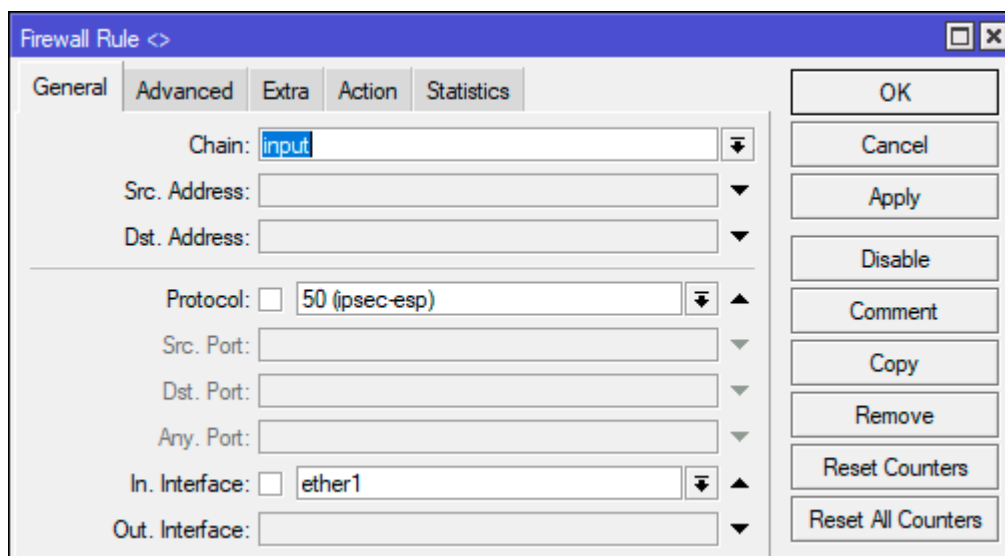
Buttons: OK, Cancel, Apply, Copy, Remove

В терминале:

```
/ip ipsec profile
set [ find default=yes ] dh-group=ecp256,ecp384,modp2048 enc-algorithm=aes-256
```

Для окончания настройки разрешим подключения к L2TP-серверу в брандмауэре. Для этого нам понадобится создать два правила, первое должно разрешать подключения для протоколов **L2TP** (порт **1701 UDP**), **IKE** (порт **500 UDP**) и протокола **NAT-T** (порт **4500 UDP**), второе для протокола **50 ESP** (*Encapsulating Security Payload*). Переходим в **IP - Firewall** и создаем первое правило: **Chain -**

input, Protocol - udp, Dst. Port - 500,1701,4500, в поле **In. Interface** указываем внешний интерфейс роутера, в нашем случае ether1. Затем второе: **Chain - input, Protocol - ipsec-esp, In. Interface -**внешний интерфейс (ether1). Так как действие по умолчанию **accept** достаточно просто сохранить правила.



Для терминала выполните следующие команды:

```
/ip firewall filter
add action=accept chain=input dst-port=500,1701,4500 in-interface=ether1
protocol=udp
add action=accept chain=input in-interface=ether1 protocol=ipsec-esp
```

На этом настройка L2TP/IPsec-сервера закончена.

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.