

Работаем с сертификатами Let's Encrypt на роутерах Mikrotik (RouterOS 7)

 interface31.ru/tech_it/2023/07/rabotaem-s-sertifikatami-lets-encrypt-na-routerah-mikrotik-routeros-7.html

Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Работаем с сертификатами Let's Encrypt на роутерах Mikrotik (RouterOS 7)

Рассказывать о том, что такое Let's Encrypt сегодня не нужно, этот центр сертификации стал фактически стандартом де-факто для быстрого и автоматического получения бесплатных сертификатов. Это позволяет без лишних затрат надежно защитить сетевые службы и больше не возвращаться к этому вопросу. В новой версии RouterOS 7 также появилась возможность работать с этим центром сертификации, что сделало возможным отказаться от выпуска собственных сертификатов и избежать необходимости их ручной установки на клиенте. Но не все так просто и радужно и в данной статье мы эти вопросы разберем.



Онлайн-курс по MikroTik

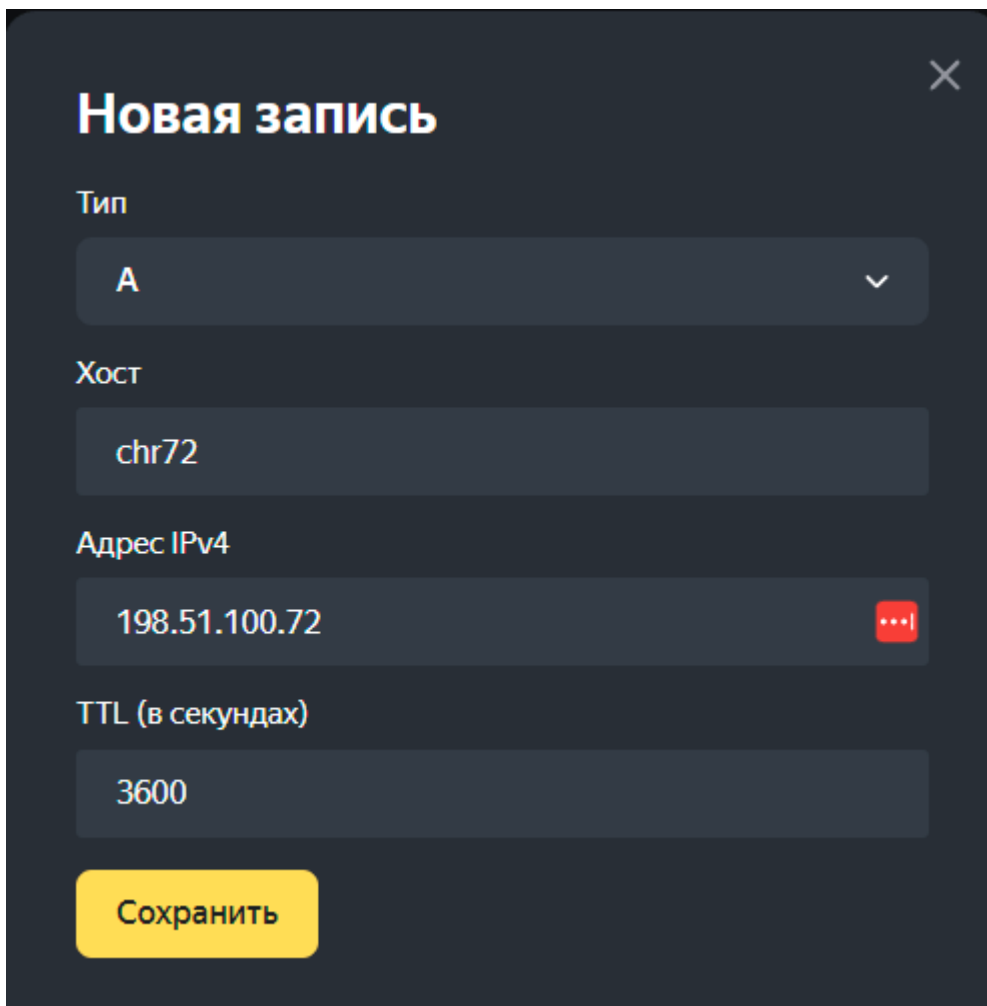
Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три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

Подготовка к получению сертификата

Для получения сертификата Let's Encrypt вам понадобится доменное имя и выделенный IP-адрес, если у вас уже есть собственный домен, то можете создать нужный поддомен и в А-записи для него указать выделенный адрес роутера. Эти изменения вносятся на DNS-сервере, обслуживающем ваш домен. Например, запись может выглядеть так (формат BIND):

```
chr72    IN A 198.51.100.72
```

При работе через веб-интерфейс смысл остается примерно тем же:



Новая запись

Тип

A

Хост

chr72

Адрес IPv4

198.51.100.72

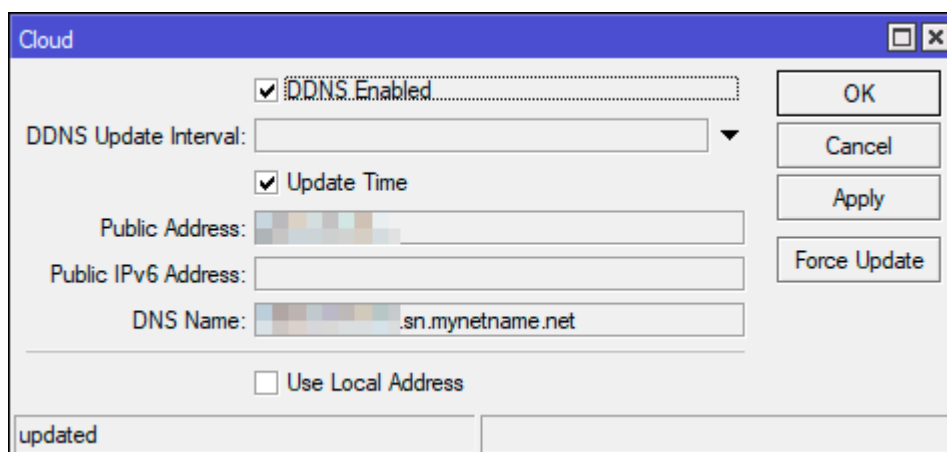
TTL (в секундах)

3600

Сохранить

Кстати, мы нигде выше не указывали сам домен. Почему? Потому что мы используем относительные записи, без точки на конце, которые затем будут дополнены именем домена? в зону которого мы вносим изменения. Так, если наш домен **example.com**, то созданная нами запись будет соответствовать **chr72.example.com**.

Если собственного доменного имени нет или выделенный адрес является динамическим, то можно использовать встроенную службу DDNS в Mikrotik. Для этого перейдите в **IP - Cloud** и установите флаг **DDNS Enabled**, через некоторое время вы получите уникальное доменное имя для роутера.



Cloud

☒ DDNS Enabled

DDNS Update Interval: [dropdown]

☒ Update Time

Public Address: [blurred IP]

Public IPv6 Address: [empty]

DNS Name: [blurred] .sn.mynetname.net

☐ Use Local Address

updated

OK

Cancel

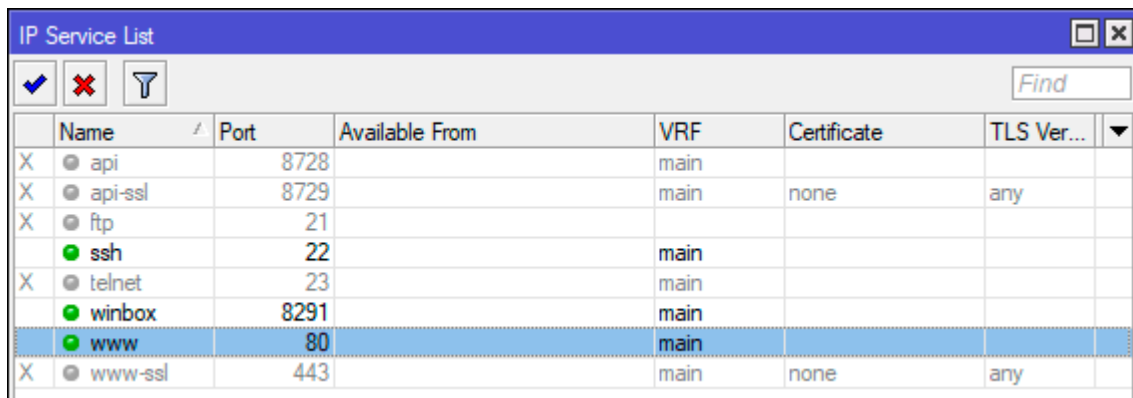
Apply

Force Update

Либо выполните в терминале:

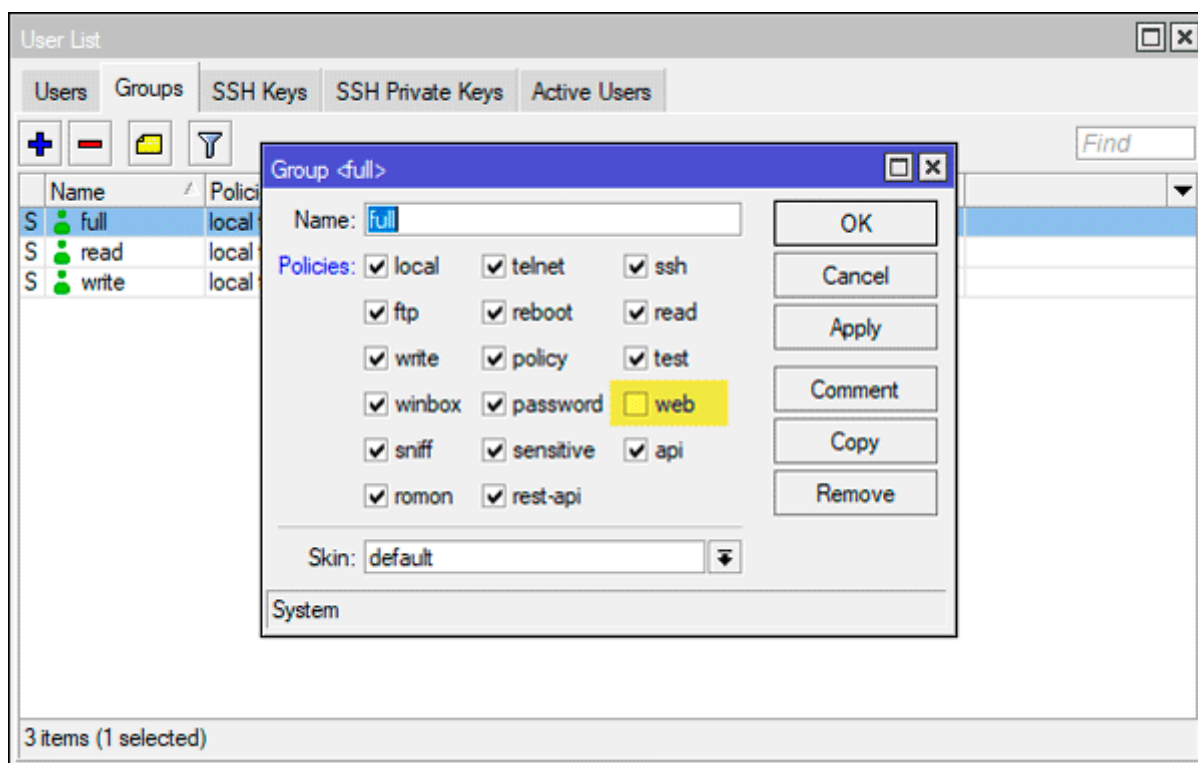
```
/ip cloud  
set ddns-enabled=yes
```

Для работы с Let's Encrypt нам потребуется веб-сервер и открытый для доступа извне 80 TCP порт. А вот здесь начинаются первые особенности, веб-сервер в RouterOS неразрывно связан с **webfig**, т.е. веб-интерфейсом для настройки роутера и вам придется его включить в **IP - Services**:



	Name	Port	Available From	VRF	Certificate	TLS Ver...
X	api	8728		main		
X	api-ssl	8729		main	none	any
X	ftp	21				
	ssh	22		main		
X	telnet	23		main		
	winbox	8291		main		
	www	80		main		
X	www-ssl	443		main	none	any

Поэтому, прежде чем открывать доступ, убедитесь, что все ваши пользователи имеют надежные пароли. Также можно подстраховаться и запретить вход в **webfig** всем или выбранным категориям пользователей. Для этого перейдите в **System - Users** и в открывшемся окне, на вкладке **Groups** для всех или только выбранных групп снимите в разрешениях флаг **web**.

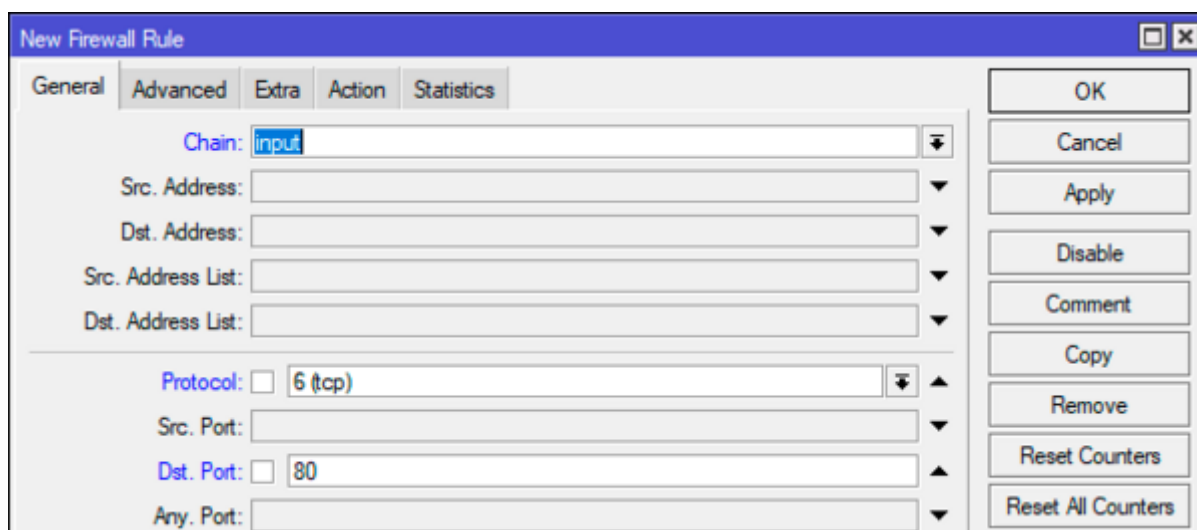


Теперь при попытке входа, даже с правильными учетными данными, вы получите сообщение что аутентификация не выполнена.



The image shows the Mikrotik RouterOS v7.8 WebFig login interface. At the top right is the Mikrotik logo. Below it, the text "RouterOS v7.8" is displayed. A warning message states: "You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator." The "WebFig Login:" section contains a "Login:" field with the text "admin" and a "Password:" field with masked characters. A "Login" button is to the right. Below the password field, a red error message reads: "Authentication failed: invalid username or password." At the bottom, there are four icons: "Winbox" (a computer monitor), "Graphs" (a green square), "License" (a document), and "Help" (a lifebuoy). The Mikrotik copyright notice is at the bottom right.

Все, что нам осталось - это создать разрешающее правило для входящего трафика на 80 порт. Переходим в **IP - Firewall** и создаем правило: **Chain - input, Protocol - 6 (tcp), Dst. Port - 80**. Так как действие по умолчанию - **accept**, то никаких дополнительных действий делать не нужно. После создания обязательно добавьте ему комментарий, например, HTTP.



The image shows the "New Firewall Rule" dialog box in Mikrotik WinBox. The "General" tab is selected. The "Chain" dropdown is set to "input". The "Protocol" dropdown is set to "6 (tcp)". The "Dst. Port" field is set to "80". The "Action" tab is also visible, showing "accept" as the default action. On the right side, there are buttons for "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", "Remove", "Reset Counters", and "Reset All Counters".

Либо в терминале:

```
/ip firewall filter
add action=accept chain=input comment=HTTP dst-port=80 protocol=tcp
```

Данное правило должно располагаться ниже правила разрешающего уже установленные и связанные соединения и выше запрещающего правила в цепочке INPUT.

Получаем сертификаты штатными инструментами RouterOS 7

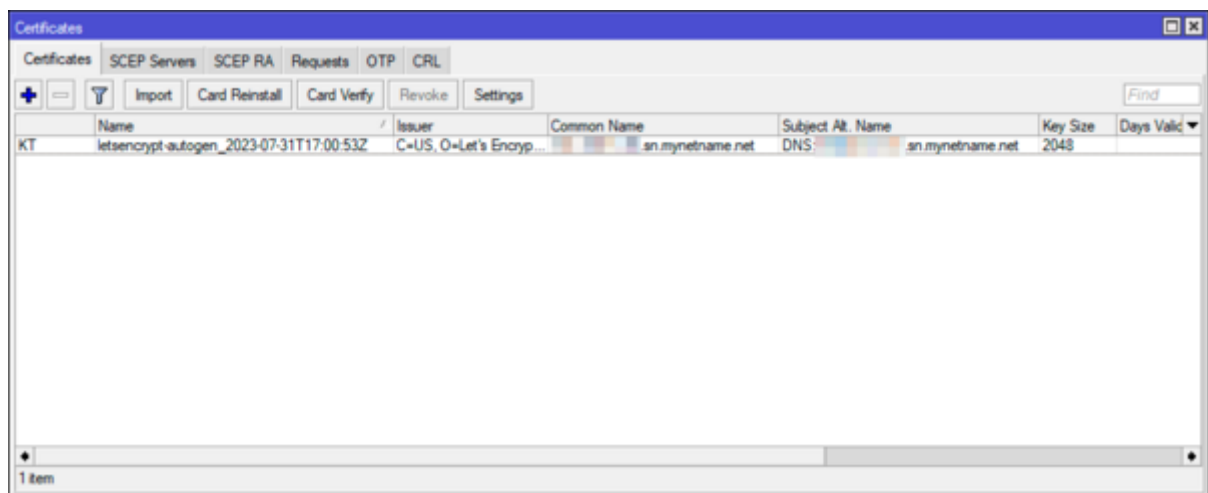
Графического инструмента для работы с Let's Encrypt нет, поэтому перейдем в терминал и отдадим команду:

```
/certificate enable-ssl-certificate dns-name=chr72.example.com
```

Если вы используете встроенную службу DDNS, то можно ограничиться командой:

```
/certificate enable-ssl-certificate
```

Полученный сертификат можно увидеть в **System - Certificates**, он будет иметь имя вроде **letsencrypt-autogen_2023-07-31T17:09:41Z** и флаги **KT**.



Он автоматически привязывается к службе **www-ssl** и также будет автоматически продляться без участия пользователя. При этом никто не мешает нам использовать данный сертификат для любых других служб, скажем - SSTP-сервера. Но здесь появляется проблема: после продления сертификат будет сохранен с новым именем (как можно было видеть выше в имя входят дата и время выпуска) и вам придется вручную изменять сертификат в настройках сервиса.

Получаем сертификаты при помощи скрипта

В общем Mikrotik в своем репертуаре: инструмент нужный и полезный, но реализация - как всегда, через одно место. Поэтому снова призовем на помощь универсальный инструмент - скрипты. С их помощью мы решим две проблемы: закроем доступ к webfig, который будем открывать только на время получения сертификата, и автоматически привяжем новый сертификат к нужным службам, в нашем примере будем использовать SSTP.

Сначала приведем полный текст, затем разберем его подробнее:

```

:log info "LE renewal"

:local DomainName "chr72.example.com"

/ip firewall filter
enable [find where comment="HTTP"]

/certificate
remove [find where common-name=$DomainName]
enable-ssl-certificate dns-name=$DomainName

:delay 60s

/certificate
:local certName [get [find where common-name=$DomainName] name]

/interface sstp-server server
:set certificate=$certName

/ip firewall filter
disable [find where comment="HTTP"]

```

Первой строкой мы делаем запись в лог со статусом info, содержимое - на собственное усмотрение. Второй - задаем доменное имя, на которое будем получать сертификат, его следует указать даже если вы используете DDNS, так как потом по нему мы будем искать нужный сертификат в хранилище.

Затем мы включаем разрешающее правило для входящего трафика на порт TCP 80, для поиска правила используется комментарий, в нашем случае HTTP.

После чего находим и удаляем старый сертификат и получаем новый, после чего берем паузу на минуту для завершения всех процессов с помещением сертификата в хранилище.

Следующим шагом определяем имя полученного сертификата и подключаем его к службе, в данном случае SSTP.

Последним шагом выключаем правило брандмауэра, открывающее доступ к веб-серверу и **webfig**.

Сертификаты Let's Encrypt выдаются сроком на 90 дней, поэтому следует запускать данный скрипт немного раньше, скажем раз в 85 дней, чтобы в случае чего у вас было время на анализ и исправление ситуации.

Надеемся, что данная статья будет вам полезна и поможет начать работать с сертификатами Let's Encrypt на роутерах Mikrotik.

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.
