Let's Encrypt на MikroTik: настройка и продление сертификата для IKEv2 VPN

Let's Encrypt на MikroTik: настройка и продление сертификата для IKEv2 VPN

Введение

Для работы IKEv2 VPN с проверкой подлинности сервера используется TLS-сертификат. Если сертификат просрочен, не соответствует доменному имени или клиент не может проверить цепочку доверия, подключение может завершиться ошибкой аутентификации.

В RouterOS предусмотрена поддержка ACME, позволяющая получать и продлевать сертификаты Let's Encrypt непосредственно на MikroTik.

В этой статье рассмотрим общий порядок настройки, проверки и продления сертификата для IKEv2 VPN.

Оборудование и программное обеспечение:

- MikroTik RouterOS 7.x с поддержкой ACME.
- Let's Encrypt.
- IKEv2 VPN.
- Клиент strongSwan для Android в качестве примера проверки.

Команды и названия отдельных параметров могут отличаться в зависимости от версии RouterOS.

1. Подготовка

Перед выпуском сертификата необходимо подготовить доменное имя и проверить сетевую доступность устройства.

Требования

1. Доменное имя должно указывать на публичный IP-адрес MikroTik.
2. На маршрутизаторе должны быть настроены IPsec и IKEv2.
3. Для проверки HTTP-01 должен быть доступен TCP-порт 80.
4. В Firewall должно быть разрешено входящее подключение к порту 80 со стороны WAN.
5. HTTP-сервис MikroTik должен поддерживать ACME-проверку.

Проверить состояние HTTP-сервиса:

```
/ip service print
```

Проверить правила Firewall:

```
/ip firewall filter print detail
```

Важно убедиться, что разрешающее правило для TCP/80 расположено выше общего правила блокировки входящих подключений с WAN.

2. Выпуск сертификата Let's Encrypt

Для выпуска сертификата используется встроенная команда ACME:

```
/certificate add-acme directory-url=https://acme-v02.api.letsencrypt.org/directory domain-names=vpn.example.com name=ikev2-cert
```

В команде необходимо заменить:

- `vpn.example.com` — собственным доменным именем;
- `ikev2-cert` — произвольным понятным именем сертификата.

После выполнения команды маршрутизатор обращается к Let's Encrypt, проходит проверку домена и получает сертификат.

Проверить результат:

```
/certificate print detail where name="ikev2-cert"
```

У успешно выпущенного сертификата должны присутствовать:

- `K` — приватный ключ;
- `a` — сертификат управляется ACME.

Также необходимо проверить Common Name, Subject Alternative Name и срок действия сертификата.

3. Настройка цепочки сертификатов для IKEv2

Для корректной проверки серверного сертификата клиенту необходима доверенная цепочка сертификатов.

В зависимости от используемой цепочки Let's Encrypt она может включать:

- конечный сертификат домена;
- промежуточный сертификат удостоверяющего центра;
- корневой сертификат.

На MikroTik необходимо убедиться, что нужные сертификаты присутствуют в хранилище.

Посмотреть список:

```
/certificate print detail
```

При настройке IPsec identity указывается серверный сертификат и необходимые сертификаты цепочки.

Пример:

```
/ip ipsec identity set [find where peer="ikev2-peer"] certificate="ikev2-cert,intermediate-ca,root-ca"
```

Названия промежуточного и корневого сертификатов в примере условные. Используйте фактические имена сертификатов из хранилища и проверяйте соответствие цепочки.

Не следует без необходимости изменять настройки других IPsec identity: на одном маршрутизаторе могут работать несколько независимых VPN-подключений.

4. Проверка подключения

После назначения сертификата необходимо проверить подключение с клиентского устройства.

В Android можно использовать strongSwan.

При успешной проверке в журнале strongSwan должны присутствовать сообщения, подтверждающие:

- получение конечного сертификата сервера;
- построение цепочки до доверенного корневого сертификата;
- успешную проверку серверной RSA-подписи;
- переход к следующему этапу аутентификации EAP, если используется EAP.

Пример сообщения:

```
authentication of 'CN=vpn.example.com' with RSA signature successful
```

Это означает, что клиент успешно проверил серверную подпись. Однако это ещё не гарантирует успешную аутентификацию пользователя: логин и пароль проверяются отдельно на этапе EAP.

Если после успешной проверки сертификата появляется `EAP authentication failed`, следует отдельно проверять учётные данные и настройки RADIUS или User Manager.

5. Автоматическое продление сертификата

RouterOS поддерживает автоматическое продление ACME-сертификатов.

Обычно автоматическое обновление запускается после истечения примерно 80% срока действия сертификата.

Для контроля рекомендуется периодически проверять срок действия:

```
/certificate print detail where name="ikev2-cert"
```

Также можно посмотреть состояние ACME:

```
:put [/certificate/get [find where name="ikev2-cert"] acme-status]
```

Если автоматическое обновление не произошло, можно выполнить ручное продление:

```
/certificate/acme-renew ikev2-cert
```

После завершения необходимо повторно проверить:

- срок действия;
- наличие приватного ключа;
- статус ACME;
- привязку сертификата к IPsec identity.

Не нужно удалять действующий сертификат и создавать новый при каждом продлении.

6. Безопасность: закрытие TCP/80

При использовании HTTP-01 Let's Encrypt необходимо временно обеспечить доступ к TCP/80 для проверки домена.

После успешного выпуска или продления сертификата рекомендуется вернуть исходные ограничения:

1. Отключить HTTP-сервис, если он не нужен для других задач.
2. Отключить разрешающее правило Firewall для TCP/80, если оно открывалось только ради ACME.
3. Проверить, что другие необходимые сервисы не затронуты.

Пример:

```
/ip service disable www
```

Правило Firewall следует отключать по его фактической конфигурации, а не по условному номеру из примера.

Важный нюанс: если автоматическое продление использует HTTP-01, закрытый порт 80 может помешать следующей проверке Let's Encrypt. Поэтому необходимо заранее проверить, как будет обеспечиваться доступ во время автоматического продления. Если требуется временное открытие порта, его нужно согласовать с выбранным способом обновления.

7. Диагностика типичных проблем

Симптом	Что проверить
ACME не выпускает сертификат	DNS, доступность TCP/80, Firewall, HTTP-сервис
Сертификат выпущен, но клиент его не принимает	Имя домена, SAN, срок действия, цепочку доверия
`signature validation failed`	Соответствие сертификата и приватного ключа, актуальность сертификата, алгоритм подписи
Серверная подпись проверена, но VPN не подключается	EAP, логин/пароль, RADIUS или User Manager
Автоматическое продление не работает	ACME status, доступность HTTP-01, журналы RouterOS

При диагностике важно разделять две независимые стадии:

- **Проверка сертификата сервера** — подтверждает подлинность VPN-сервера.
- **Аутентификация пользователя** — проверяет право конкретного пользователя на подключение.

Успешное прохождение первой стадии не означает автоматического успеха второй.

8. Рекомендации по эксплуатации

- Используйте отдельный сертификат для VPN, если на устройстве работают другие сервисы с собственными сертификатами.
- Не удаляйте старый сертификат до проверки нового.
- Не изменяйте рабочие IPsec identity без необходимости.
- Контролируйте сроки действия сертификатов.
- Проверяйте результат продления с реального клиентского устройства.
- Не оставляйте TCP/80 открытым, если он не требуется для текущего способа проверки.
- Сохраняйте рабочую конфигурацию и документируйте изменения.

Заключение

Встроенная поддержка ACME в MikroTik позволяет получать и продлевать Let's Encrypt-сертификаты без отдельного сервера сертификации.

При правильной настройке DNS, Firewall, HTTP-01 и IPsec identity обслуживание сертификатов становится достаточно простым. Главное — контролировать срок действия, проверять результат обновления и не путать ошибки сертификатной проверки с ошибками пользовательской аутентификации.

Полезные ссылки:

- Официальная документация MikroTik — Certificates
- Let's Encrypt — документация
- strongSwan — документация

Revision #1
Created 2026-11-20 18:26:56 UTC by im
Updated 2026-11-20 18:27:10 UTC by im