

Настройка SSTP VPN-сервера на роутерах Mikrotik

 interface31.ru/tech_it/2021/05/nastroyka-sstp-vpn-servera-na-routerah-mikrotik.html

Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Настройка SSTP VPN-сервера на роутерах Mikrotik

Продолжая тему VPN для удаленного доступа, сегодня мы хотим рассмотреть настройку SSTP-сервера на базе оборудования Mikrotik. Это не самый распространенный и популярный протокол, но имеющий ряд особенностей и преимуществ, главное из которых - использование стандартного протокола HTTPS для установления соединения, что делает SSTP-трафик неотличимым от обычного и дает возможность работать из любой точки, где есть интернет, проходя через NAT, брандмауэры и даже прокси-сервера. При этом его достаточно просто настроить и использовать, о чем мы расскажем 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.

Практически все из рассмотренных нами ранее протоколов VPN имеют те или иные ограничения, которые могут помешать установить соединение в условиях ограниченного доступа к сети интернет. Особенно это актуально для публичных и гостиничных сетей, где может быть заблокировано практически все, кроме обычного HTTP/HTTPS. Именно в таких сценариях раскрываются сильные стороны протокола SSTP и отходят на второй план слабые. Как мы уже говорили раньше - нет универсального VPN-решения, каждое из них имеет свои особенности и недостатки, поэтому для каждой задачи надо выбирать именно то, что поможет решить ее наилучшим образом.

SSTP, как технологию удаленного доступа следует рассматривать в первую очередь для тех клиентов, которые могут работать из самых различных мест и должны всегда иметь возможность быстро подключиться к корпоративной сети соблюдая высокие требования безопасности. К недостаткам следует отнести повышенные накладные расходы и связанную с этим невысокую производительность, но это общий недостаток всех VPN-протоколов поверх TCP.

В случае использования оборудования Mikrotik встает вопрос высокой нагрузки на процессор для моделей без аппаратной поддержки AES. При этом вне зависимости от аппаратной поддержки шифрования скорость канала для недорогих моделей вряд-ли превысит 20-25 МБит/с , вне зависимости от доступной ширины канала. Более подробно об этом можете прочитать в нашей статье [Производительность младших моделей Mikrotik hEX и hAP. Экспресс-тестирование](#). Поэтому мы не советуем использовать SSTP для каналов, предполагающих высокую загрузку, но можем рекомендовать как надежное и безопасное средство удаленного доступа для сотрудииков, часто работающих вне стационарных рабочих мест.

Создание центра сертификации и выпуск сертификатов

Так как SSTP использует HTTPS для установления защищенного соединения нам понадобится сертификат сервера, поэтому создадим собственный центр сертификации (CA) и выпустим необходимый сертификат. Если в вашей сети уже имеется развернутая инфраструктура PKI, то можете выпустить сертификат с ее помощью, мы же рассмотрим использование для этих целей собственных возможностей RouterOS.

Перед тем, как приступить к созданию центра сертификации убедитесь, что на роутере правильно настроено текущее время и часовой пояс, а также включена синхронизация времени через NTP.

Сначала выпустим **корневой сертификат**, для этого перейдем в **System - Certificate** и создадим новый сертификат заполнив поля как указано на рисунке, красным обозначены обязательные к заполнению.

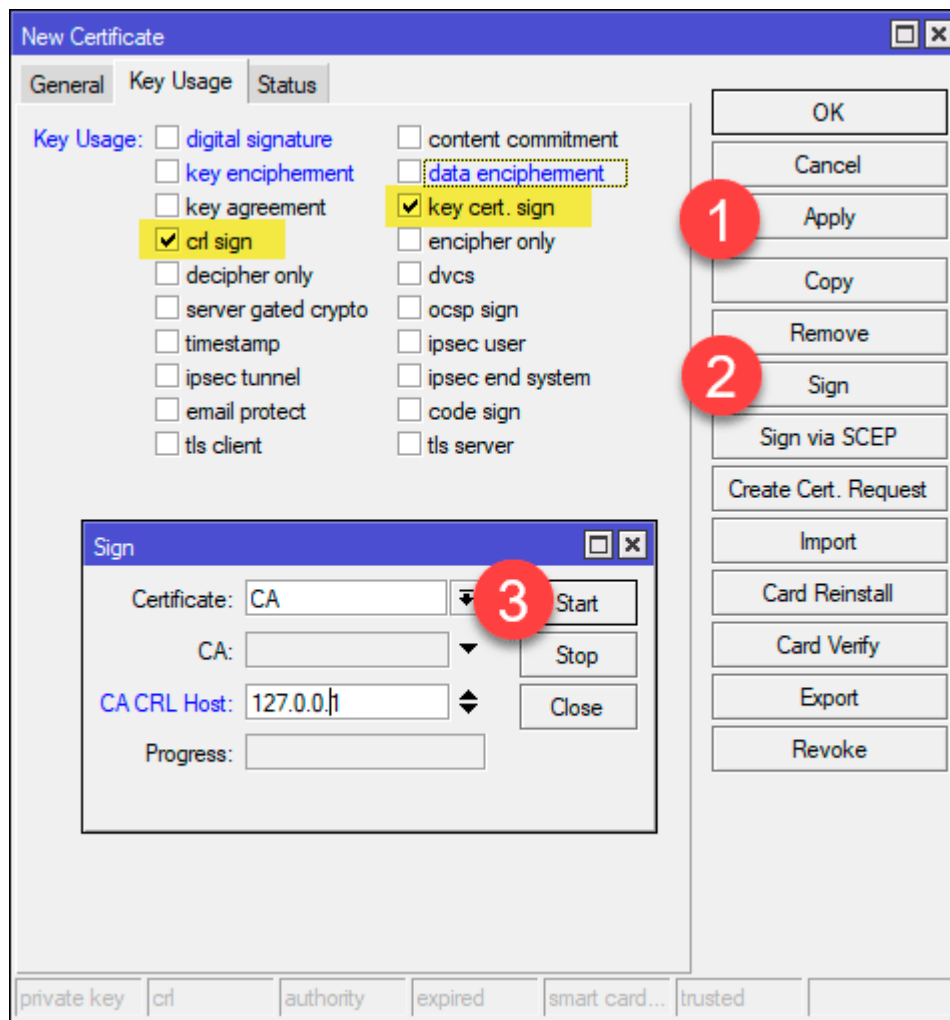
The image shows a 'New Certificate' dialog box with the following fields and values:

- Name:** CA
- Country:** RU
- State:** 31
- Locality:** BEL
- Organization:** Interface LLC
- Unit:** IT
- Common Name:** CA
- Key Size:** 2048
- Days Valid:** 3650

The 'Key Usage' tab is also visible, showing the following options: private key, crl, authority, expired, smart card..., and trusted.

Name - видимое имя сертификата, **Common Name** - имя субъекта, которому выдан сертификат, в каждом из них указываем CA (т.е. *Certification authority*). Вообще там можно написать все что угодно, но правила хорошего тона требуют давать сертификатам понятные имена. **Key Size** - размер ключа, оставляем по умолчанию 2048, **Days Valid** - срок действия сертификата в днях, имеет смысл указать достаточно продолжительный срок, в нашем случае 10 лет.

Перейдем на вкладку **Key Usage** и оставим только **crl sign** и **key cert. sign**, затем сохраним сертификат нажав **Apply**, и подпишем его кнопкой **Sign**, в открывшемся окне следует указать **CA CRL Host**, для которого можно использовать один из IP-адресов роутера, в нашем случае это localhost. Если же при помощи данного CA вы собираетесь выпускать сертификаты для других серверов, то следует указать доступный для них адрес, внутренний или внешний.



В терминале все это можно быстро сделать командами:

```
/certificate
add name=CA country="RU" state="31" locality="BEL" organization="Interface LLC"
common-name="CA" key-size=2048 days-valid=3650 key-usage=crl-sign,key-cert-sign
sign CA ca-crl-host=127.0.0.1
```

Затем выпустим сертификат сервера. При этом надо определиться каким образом вы будете подключаться к серверу по IP-адресу или FQDN (доменному имени), второй вариант более предпочтителен, так как при смене адреса вам придется перевыпустить сертификат сервера и изменить настройки всех клиентских подключений.

Заполнение полей практически ничем не отличается от предыдущего сертификата, за исключением **Common Name** и **Subject Alt. Name**, в них указываем FQDN или IP-адрес сервера, для поля **Subject Alt. Name** также указываем тип: **DNS** - для доменного имени или **IP** для адреса. Срок действия сертификата также имеет смысл сделать достаточно большим, в нашем случае 10 лет.

New Certificate

General Key Usage Status

Name: sstp.interface31.lab

Issuer:

Country: RU

State: 31

Locality: BEL

Organization: Interface LLC

Unit: IT

Common Name: sstp.interface31.lab

Subject Alt. Name: DNS : sstp.interface31.lab

Key Type:

Key Size: 2048

Days Valid: 3650

private key | crl | authority | expired | smart card key | trusted

OK

Cancel

Apply

Copy

Remove

Sign

Sign via SCEP

Create Cert. Request

Import

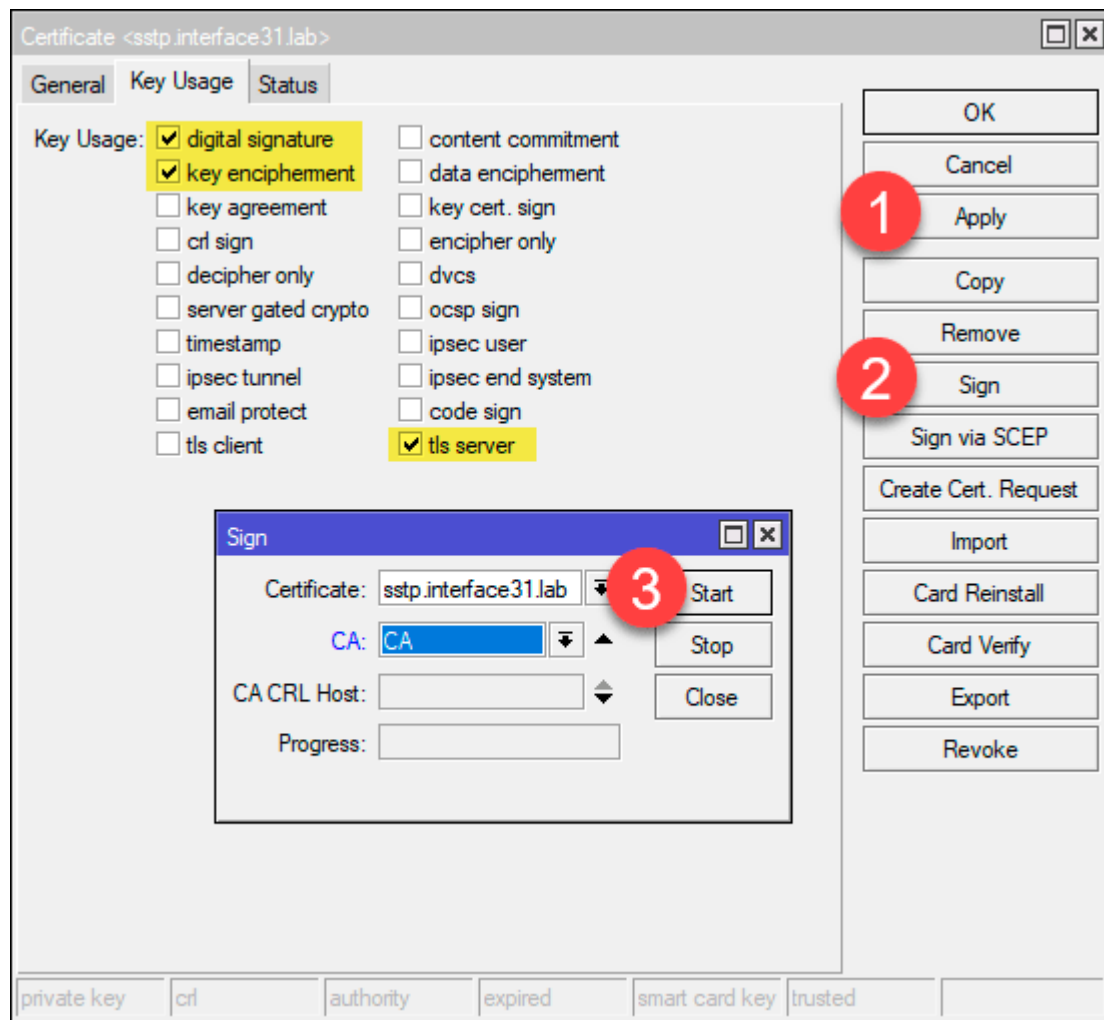
Card Reinstall

Card Verify

Export

Revoke

На закладке **Key Usage** устанавливаем **digital-signature**, **key-encipherment** и **tls-server** и подписываем сертификат сервера, для этого в поле **CA** выберите ранее выпущенный корневой сертификат.

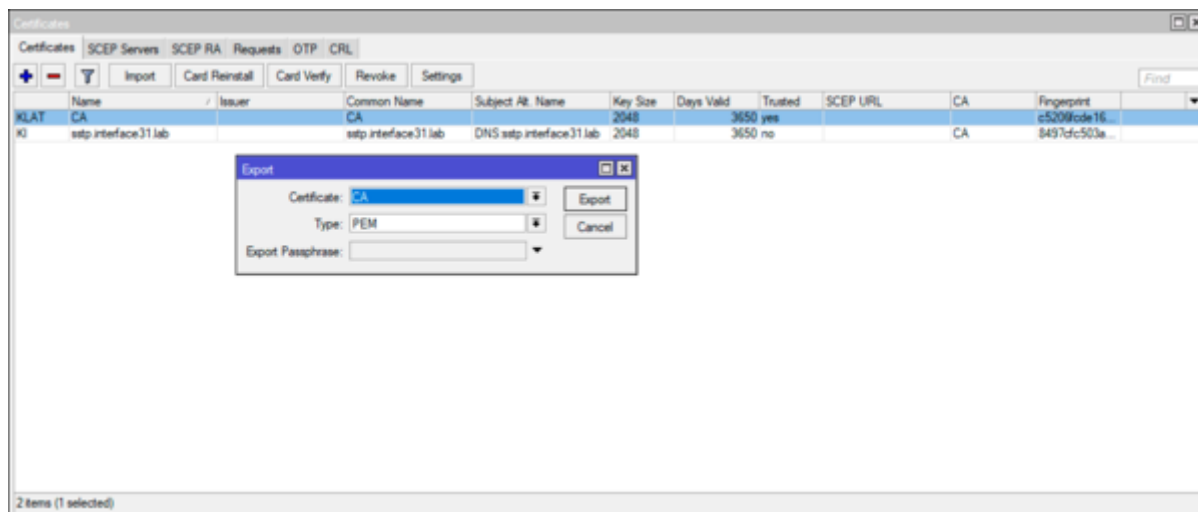


В терминале:

```
/certificate
add name=ssstp.interface31.lab country="RU" state="31" locality="BEL"
organization="Interface LLC" common-name="ssstp.interface31.lab" subject-alt-
name=DNS:"ssstp.interface31.lab" key-size=2048 days-valid=3650 key-usage=digital-
signature,key-encipherment,tls-server
sign sstp.interface31.lab ca="CA"
```

При подключении через SSTP клиент прежде всего устанавливает с сервером защищенное соединения, а для этого ему нужно проверить сертификат и убедиться в его подлинности, в противном случае продолжение соединения будет невозможным. Чтобы клиентские системы доверяли нашим сертификатам нам нужно будет установить на них корневой сертификат нашего CA.

Для этого выберем корневой сертификат в **System - Certificate**, щелкнем на нем правой кнопкой мыши и нажмем **Export**, в поле **Type** ставим **PEM**, пароль не указываем, так как нам нужен только сертификат, без закрытого ключа. Закрытый ключ центра сертификации является секретным и никогда не должен покидать пределы роутера.



В терминале сертификат можно экспортировать командой:

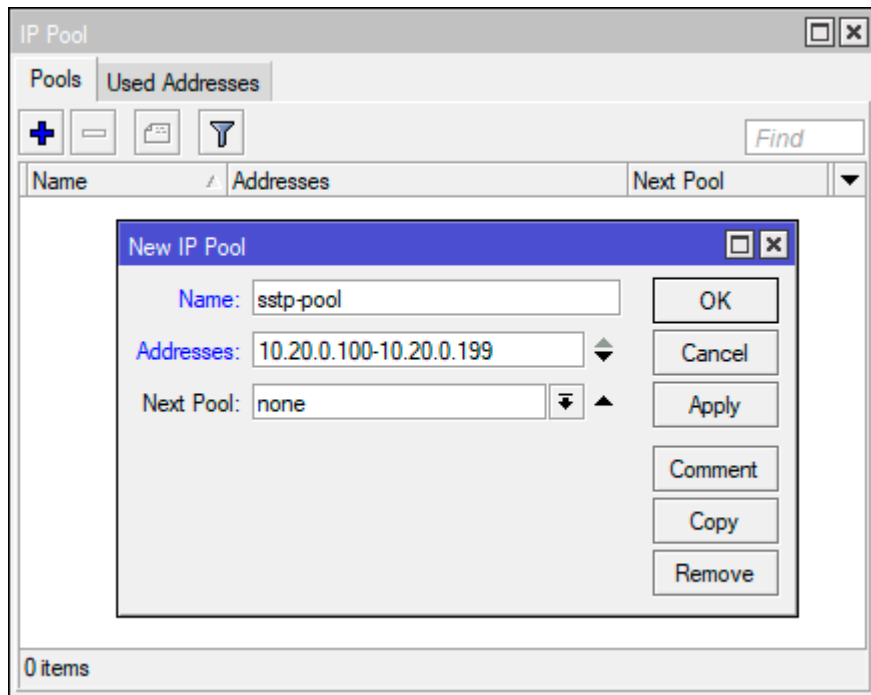
```
/certificate
export-certificate CA
```

Найти и скачать выгруженный сертификат можно в разделе **Files**.

Настройка SSTP VPN-сервера

Перед тем как браться за настройку сервера следует определиться со схемой доступа к сети, существуют два основных варианта: Proxy ARP, когда адреса удаленным клиентам выдаются **из диапазона основной сети** и они получают доступ без дополнительных настроек, и маршрутизация, когда диапазон адресов для VPN-клиентов **не пересекается с основной сетью**, а для доступа в нее будет необходимо указать маршруты, этот процесс можно автоматизировать с помощью PowerShell.

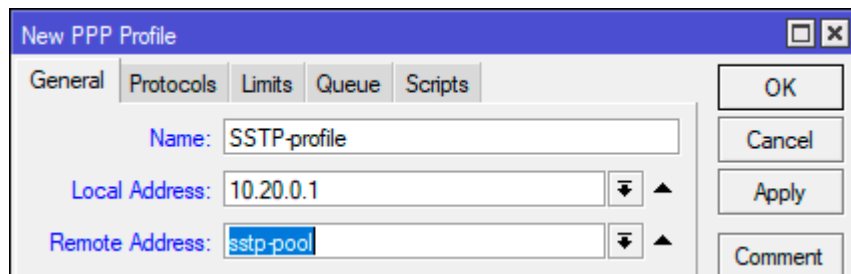
После этого перейдем в **IP - Pool** и создадим новый пул адресов для выдачи VPN-сервером, количество адресов в пуле не должно быть меньше предполагаемого количества клиентов.



В терминале:

```
/ip pool
add name=sstp-pool ranges=10.20.0.100-10.20.0.199
```

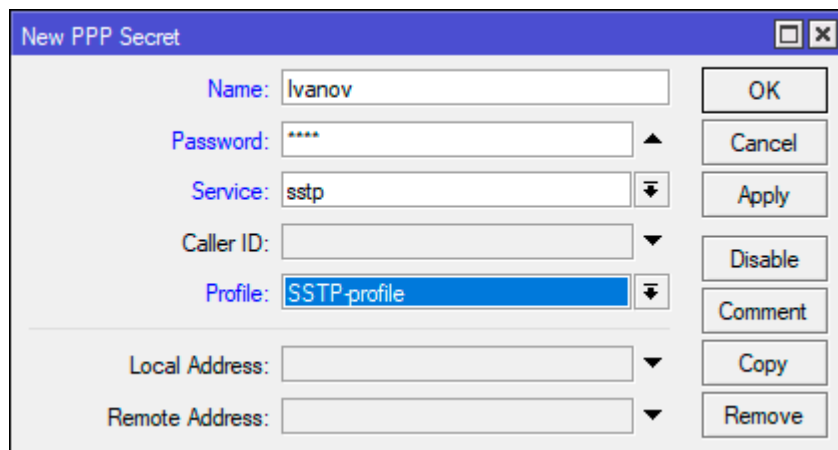
Затем перейдем в **PPP - Profiles** и создадим новый профиль, в поле **Local Address** введем локальный адрес VPN-сервера, он должен относиться к тому же диапазону что и выделенный выше пул адресов, который следует указать в поле **Remote Address**, остальные настройки оставляем по умолчанию.



Или выполним команду:

```
/ppp profile
add local-address=10.20.0.1 name=SSTP-profile remote-address=sstp-pool
```

Затем переместимся в **PPP - Secrets** и создадим учетные записи пользователей, указываем имя пользователя, пароль, в поле **Service** выбираем **sstp**, что ограничит действие учетной записи только SSTP-сервером, если оставить **any**, то учетка сможет подключаться к любому сервису. В поле **Profile** указываем созданный нами профиль.



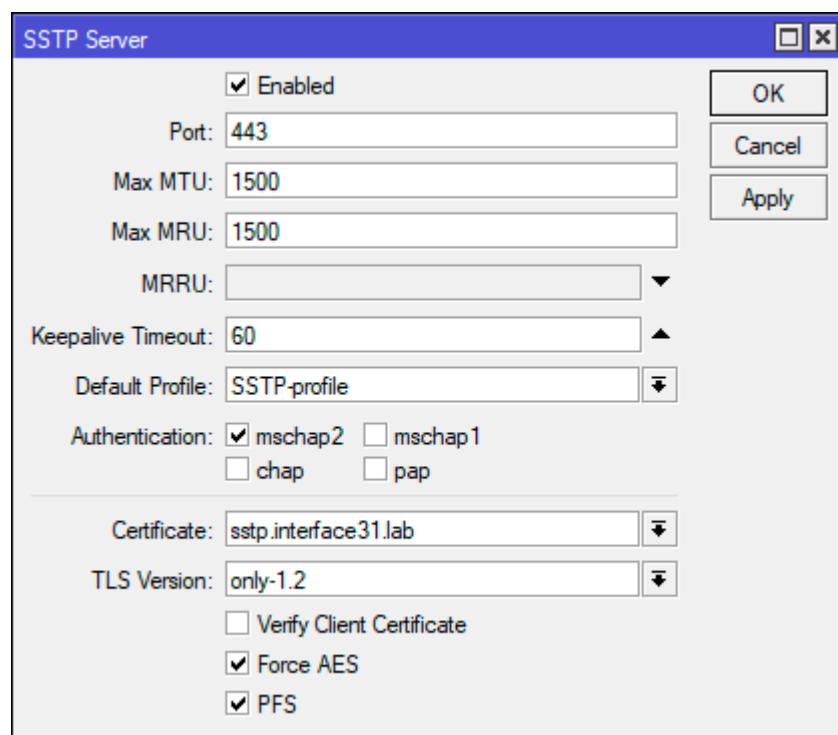
The 'New PPP Secret' dialog box contains the following fields and controls:

- Name:** Text field with 'Ivanov' entered.
- Password:** Password field with four asterisks.
- Service:** Text field with 'sstp' entered.
- Caller ID:** Text field (empty).
- Profile:** Dropdown menu with 'SSTP-profile' selected.
- Local Address:** Text field (empty).
- Remote Address:** Text field (empty).
- Buttons:** OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

Эти же действия в командной строке:

```
/ppp secret
add name=Ivanov password=Pa$$word profile=SSTP-profile service=sstp
```

Теперь, когда все готово, настроим сам сервер. Для этого перейдем в **PPP - Interface** и нажмем кнопку **SSTP Server**. Включим его, установив флаг **Enabled**, в поле **Default Profile** выберем созданный нами профиль, в разделе **Authentication** оставим только **mschap2**, в поле **Certificate** указываем сертификат сервера. Дальнейшие настройки отвечают за повышение уровня безопасности: **TLS Version - only-1.2** не разрешает использование устаревших версий TLS, **Force AES** - заставляет принудительно использовать алгоритм шифрования AES256, **PFS** включает **совершенную прямую секретность** (*Perfect forward secrecy*), которая формирует уникальный сессионный ключ для каждого подключения, что делает невозможным расшифровку сессии даже при наличии закрытого ключа.



The 'SSTP Server' configuration dialog box contains the following settings:

- Enabled:** ☒
- Port:** 443
- Max MTU:** 1500
- Max MRU:** 1500
- MRRU:** (empty)
- Keepalive Timeout:** 60
- Default Profile:** SSTP-profile
- Authentication:**
 - ☒ mschap2
 - ☐ mschap1
 - ☐ chap
 - ☐ pap
- Certificate:** sstp.interface31.lab
- TLS Version:** only-1.2
- Options:**
 - ☐ Verify Client Certificate
 - ☒ Force AES
 - ☒ PFS
- Buttons:** OK, Cancel, Apply.

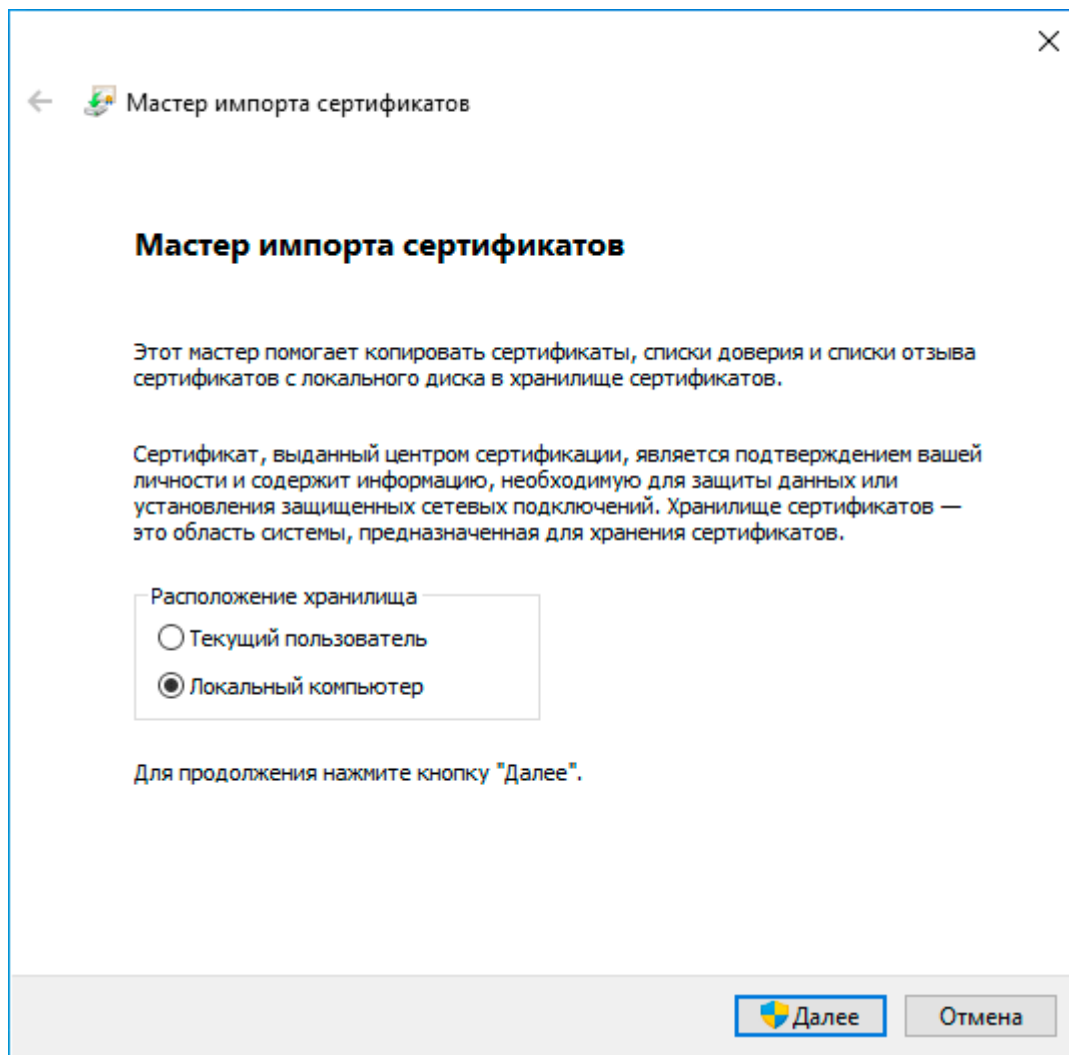
В терминале для включения и настройки сервера выполните:

```
/interface sstp-server server
set authentication=mschap2 certificate=sstp.interface31.lab default-profile=SSTP-
profile enabled=yes force-aes=yes pfs=yes tls-version=only-1.2
```

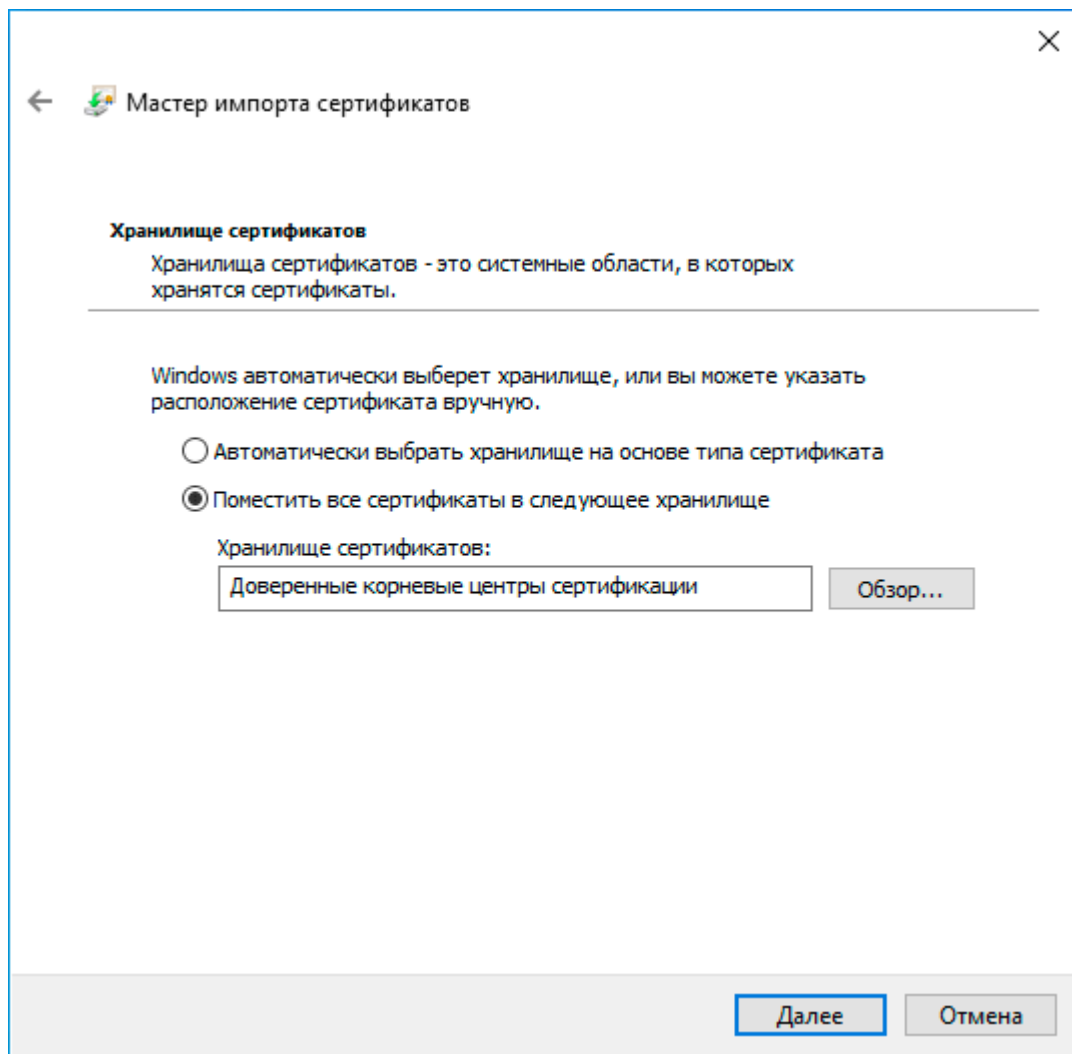
На этом настройка закончена, сервер готов принимать подключения.

Настройка подключения клиента в Windows

Как мы уже говорили, для того чтобы клиент мог проверить подлинность сервера нам необходимо импортировать корневой сертификат, переместим его на клиента и установим в **Расположение хранилища - Локальный компьютер**:



Хранилище сертификатов - Доверенные корневые центры сертификации:



Затем создаем подключение, в котором указываем **Тип VPN - Протокол SSTP** и **Тип данных для входа - Имя пользователя и пароль**, здесь же вводим адрес сервера и учетные данные.

← Параметры

Добавить VPN-подключение

Поставщик услуг VPN
Windows (встроенные)

Имя подключения
SSTP MT

Имя или адрес сервера
sstp.interface31.lab

Тип VPN
Протокол SSTP

Тип данных для входа
Имя пользователя и пароль

Имя пользователя (необязательно)
ivanov

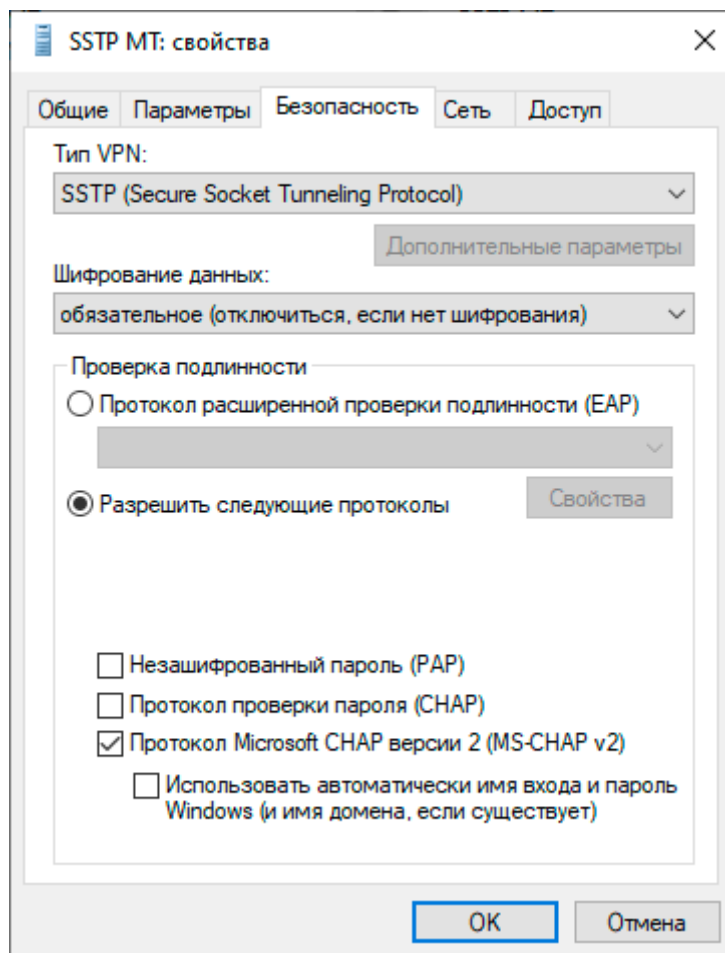
Пароль (необязательно)
•••••

☒ Запомнить мои данные для входа

Сохранить Отмена

После чего в свойствах подключения на закладке **Безопасность** убедимся, что в разделе **Проверка подлинности** указан только протокол **MS-CHAP v2**.

Настройка клиента закончена, можно подключаться.



Настройка подключения клиента в Linux

В используемых нами дистрибутивах Linux нет штатного SSTP-клиента, однако есть сторонняя разработка, которой мы и воспользуемся. Все нижесказанное будет справедливо для дистрибутивов основанных на Debian и Ubuntu, если у вас иная система обратитесь на страницу проекта.

Проще всего владельцам Ubuntu, им достаточно просто подключить PPA, ниже приведен пример для Ubuntu 18.04, для других систем просто измените кодовое название дистрибутива:

```
deb http://ppa.launchpad.net/eivnaes/network-manager-sstp/ubuntu bionic main
deb-src http://ppa.launchpad.net/eivnaes/network-manager-sstp/ubuntu bionic main
```

В Debian процесс немного более сложный, сначала получим и установим ключ репозитория проекта:

```
apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 61FF9694161CE595
```

Затем создадим файл с указанием источников пакетов:

```
touch /etc/apt/sources.list.d/sstp-client.list
```

И внесем в него следующие строки:

```
deb http://ppa.launchpad.net/eivnaes/network-manager-sstp/ubuntu eoan main
deb-src http://ppa.launchpad.net/eivnaes/network-manager-sstp/ubuntu eoan main
```

Обновим список пакетов и установим клиент:

```
apt update
apt install network-manager-sstp
```

После чего появится возможность создать SSTP-соединение штатными средствами **Network Manager**. Настройки несложные: указываем адрес сервера, учетные данные и сертификат CA, у которого предварительно следует изменить расширение на **PEM**.

The screenshot shows a window titled "Добавить VPN" (Add VPN) with three tabs: "Идентификация" (Identification), "IPv4", and "IPv6". The "Идентификация" tab is active. It contains the following fields and options:

- Название** (Name): SSTP MT
- General**
 - Шлюз** (Gateway): sstp.interface31.lab
- Optional**
 - Имя пользователя** (Username): sidorova
 - Пароль** (Password): masked with dots, with a "Показать пароль" (Show password) checkbox below it.
 - NT-домен** (NT domain): empty field
 - CA Certificate**: cert_export_CA.pem (with a file icon)
 - ☐ Ignore certificate warnings
 - ☐ Use TLS hostname extensions
- Advanced...** button with a gear icon.

Если вы все сделали правильно, то соединение будет установлено.

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.
