

1. Подготовка лабораторного стенда. Установка MikroTik CHR на VMWare

В работе приведен пример настройки стенда с виртуализацией сетевых устройств с использованием программного обеспечения VMWare, в частности, VMWare Workstation. При выполнении лабораторной работы не запрещается использовать отличное от описанного ПО, например, Oracle VirtualBox, VMWare Player, Hyper-V и другие гипервизоры, а также системы эмуляции сетевых устройств, например, GNS3 или EVE-NG, но в этих случаях некоторые шаги конфигурации лабораторного стенда могут незначительно отличаться.

1.1 Установка VMWare

В работе будем рассматривать редакцию WorkStation 15.5. Процесс установки довольно тривиальный, по принципу «next next – finish». На персональных компьютерах учебной лаборатории указанное ПО уже установлено, при использовании личного ПК необходимо скачать установочный дистрибутив (https://disk.yandex.ru/d/Hn1sq_mWJIYfiw). После установки открываем консоль управления (рис.1.1).

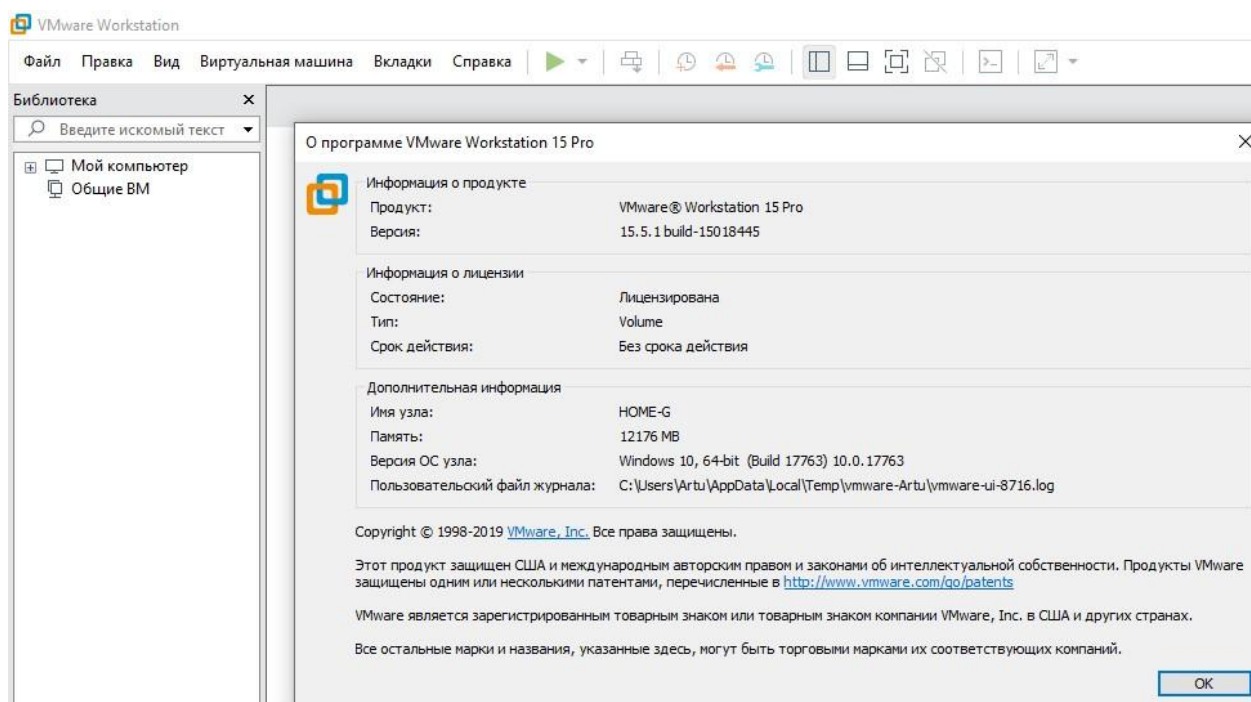


Рисунок 1.1 – Панель управления VMWare Workstation

Указанное ПО позволяет группировать виртуальные машины в отдельные категории, на рис 1.2 представлены категории BM test и Mikrotik. Отметим, что перенос ВМ между категориями не влияет на их работу и не изолирует машины друг от друга.

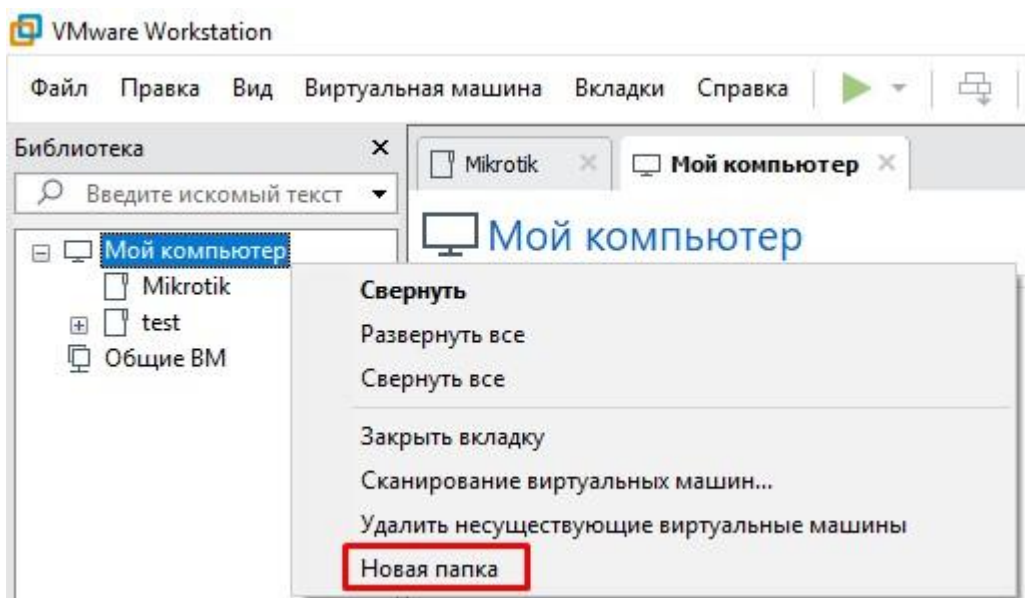


Рисунок 1.2 – Создание отдельной категории VM

1.2 Скачивание актуального образа Mikrotik CHR

Для начала работы с Mikrotik CHR понадобится получить официальный образ операционной системы устройства, доступный на сайте разработчика. Лицензия Mikrotik имеет несколько уровней, в том числе бесплатную версию без ограничения по времени использования, но имеющую ограничения на максимальную полосу пропускания сетевых интерфейсов и число VPN-туннелей.

Для скачивания образа ОС маршрутизатора, перейдем по адресу <https://mikrotik.com/download> и в разделе Cloud Hosted Router будет доступно несколько вариантов для загрузки. Наиболее новая версия RouterOS – 7.1, в ней было внесено множество изменений как в функционал, так и в производительность устройств и самой ОС, но в работе будет использоваться версия 6.48 или новее, до 7-го поколения ОС. Выбор стабильной версии обусловлен изменением ряда конфигураций в ROS и отчасти нестабильности ее работы, поэтому при загрузке рекомендуется выбрать «VMDK image 6.48.2».

Cloud Hosted Router

	6.47.9 (Long-term)	6.48.2 (Stable)
Images	vmdk, vhdx, vdi, ova, img	
Main package		
VHDX image		
VMDK image		
VDI image		Download

Рисунок 1.3 – Загрузка образа RouterOS

Для удобства можно переместить скачанный файл в C:\VMware\Mikrotik\CHR 6.48.2.vmdk

1.3 Создание виртуальной машины

Создание виртуальной машины происходит с использованием диалоговых окон ПО, первым шагом необходимо открыть консоль VMWare (стартовый экран), выбрать папку (при наличии), в которой необходимо создать новую виртуальную машину и нажать «Файл – Новая виртуальная машина». Горячая клавиша CTRL+N. Нас интересует тип установки – Выборочный.

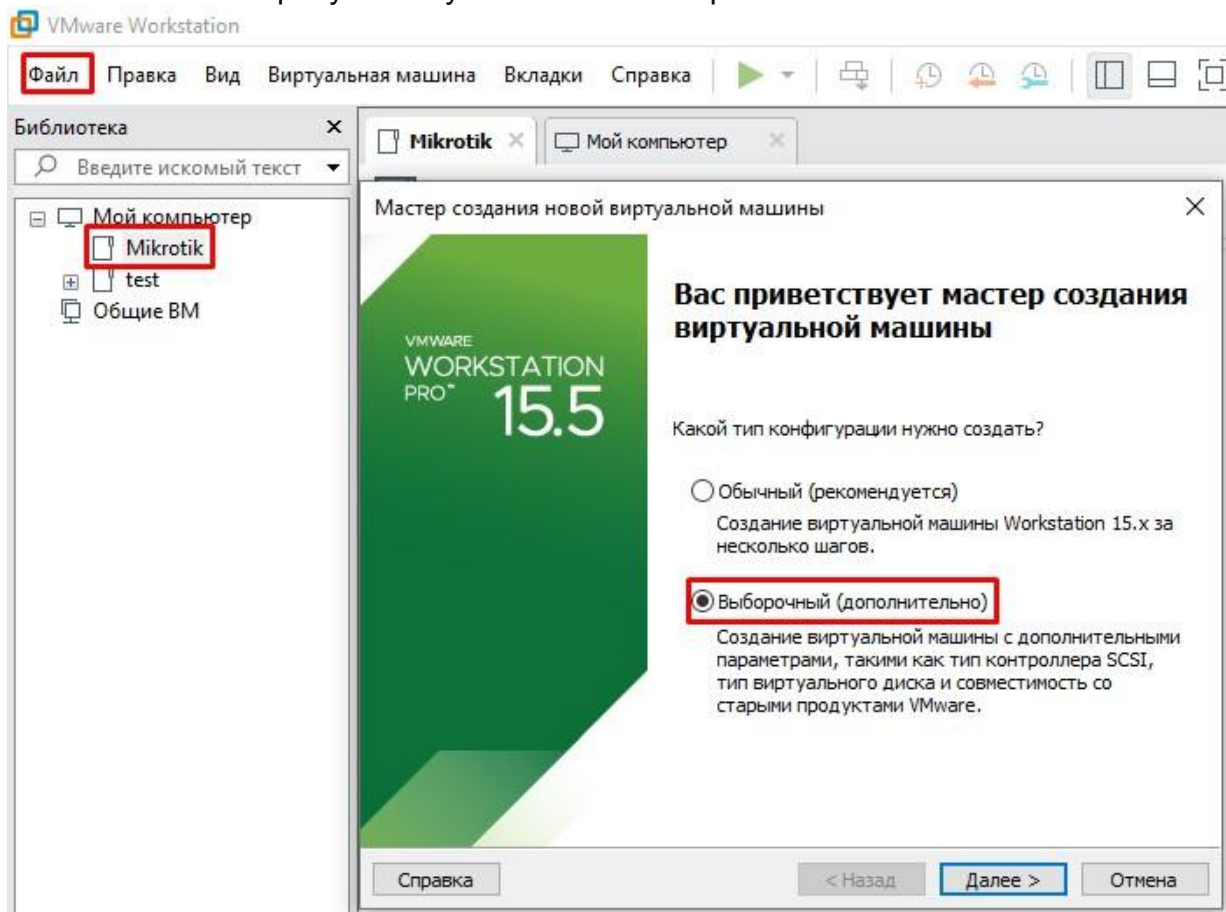


Рисунок 1.4 – Диалоговое окно создания новой ВМ

На следующем шаге выбираем совместимость аппаратного обеспечения, ничего не меняя жмём далее.

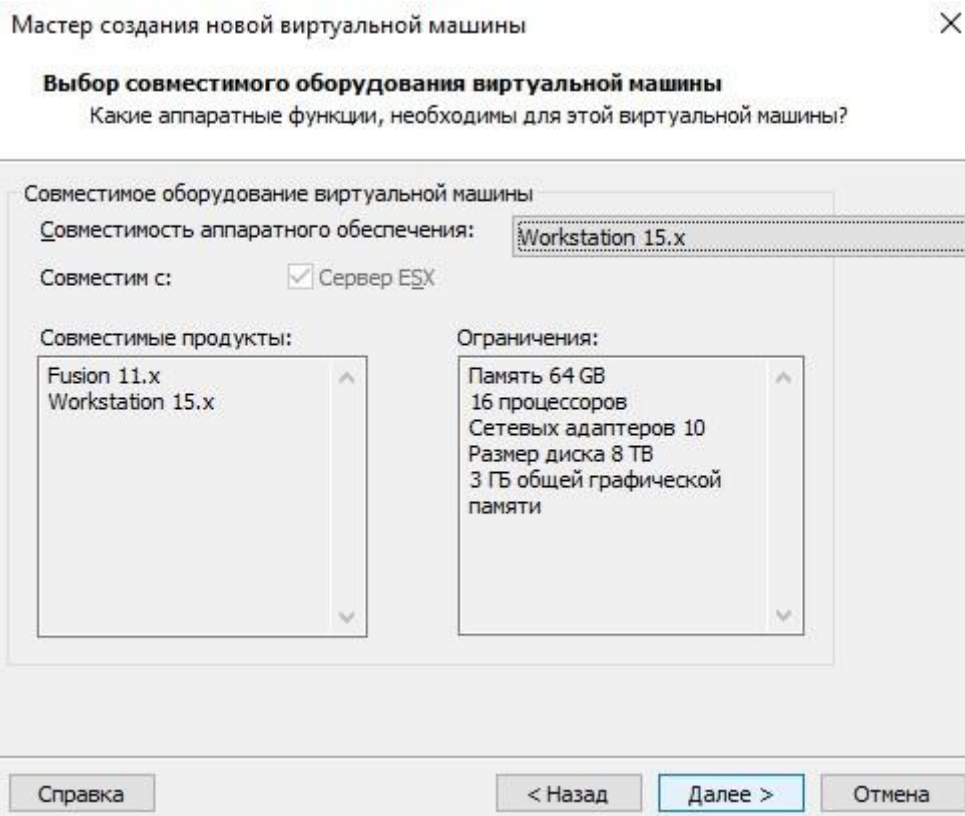


Рисунок 1.5 – Диалоговое окно создания новой ВМ

Устанавливать операционную систему на этом этапе нет необходимости, поэтому выбираем соответствующий пункт меню.

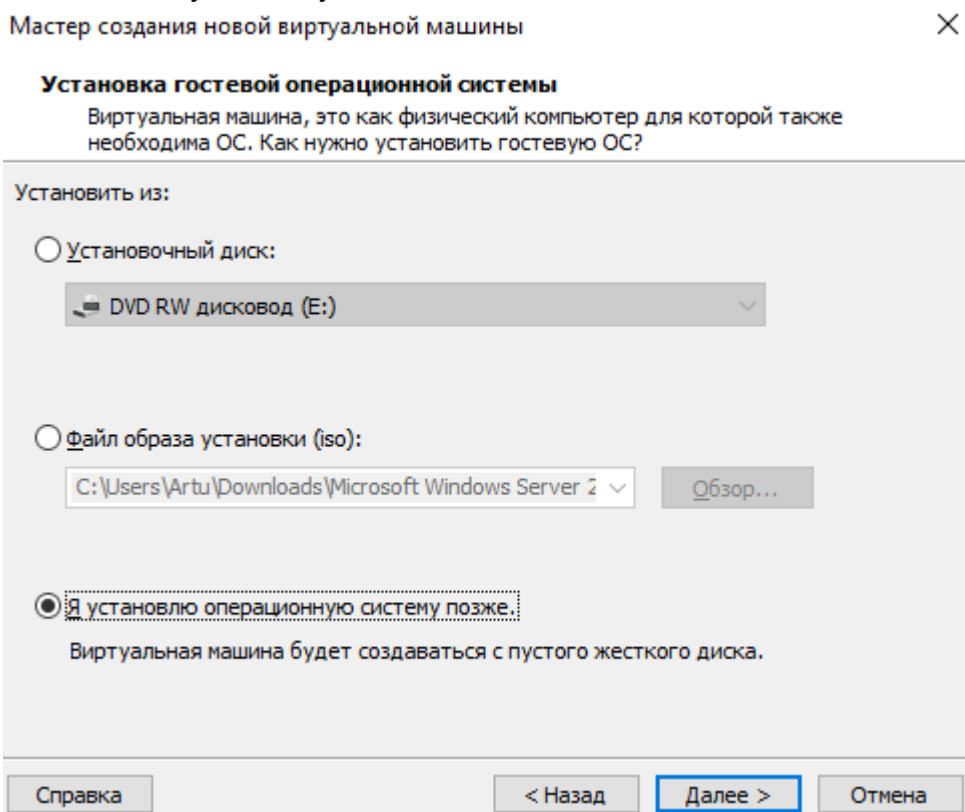


Рисунок 1.6 – Диалоговое окно создания новой ВМ

На следующем окне происходит выбор предустановленных параметров виртуальной ОС. VMWare знает конечно о многих ОС, но о CHR точно ничего, поэтому выбираем «Другая – Other 64 bit».

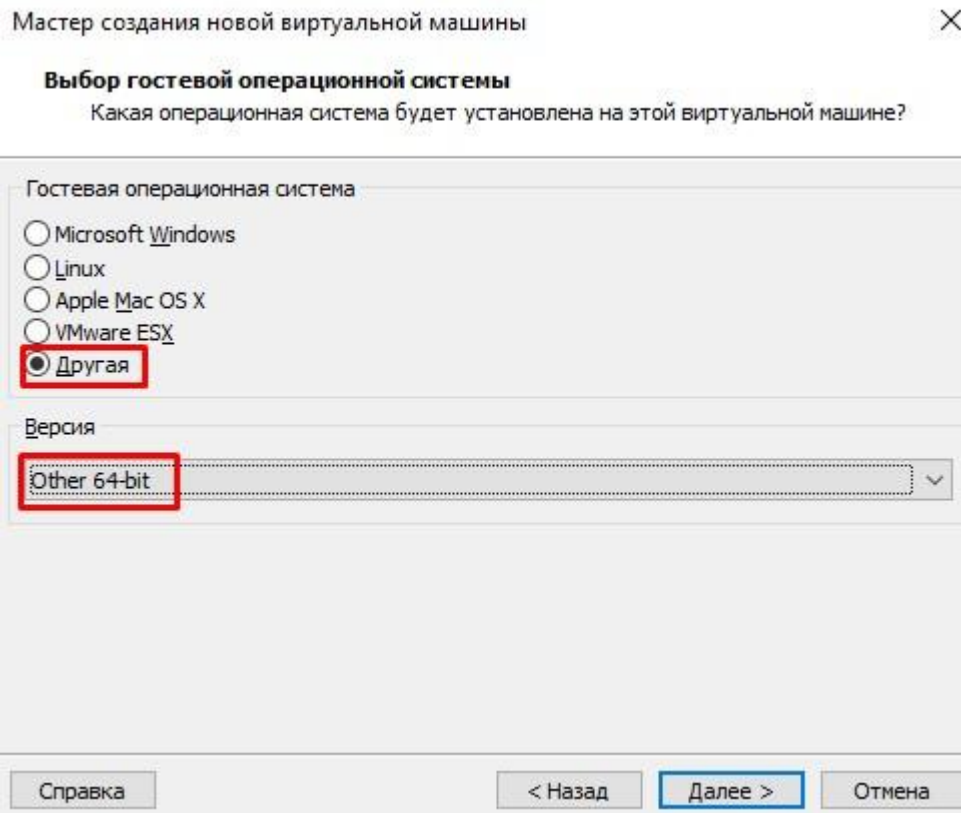


Рисунок 1.7 – Диалоговое окно создания новой VM

Задаём имя виртуальной машины и ее расположение. Игнорируем всплывающие предупреждения нажав кнопку продолжить.

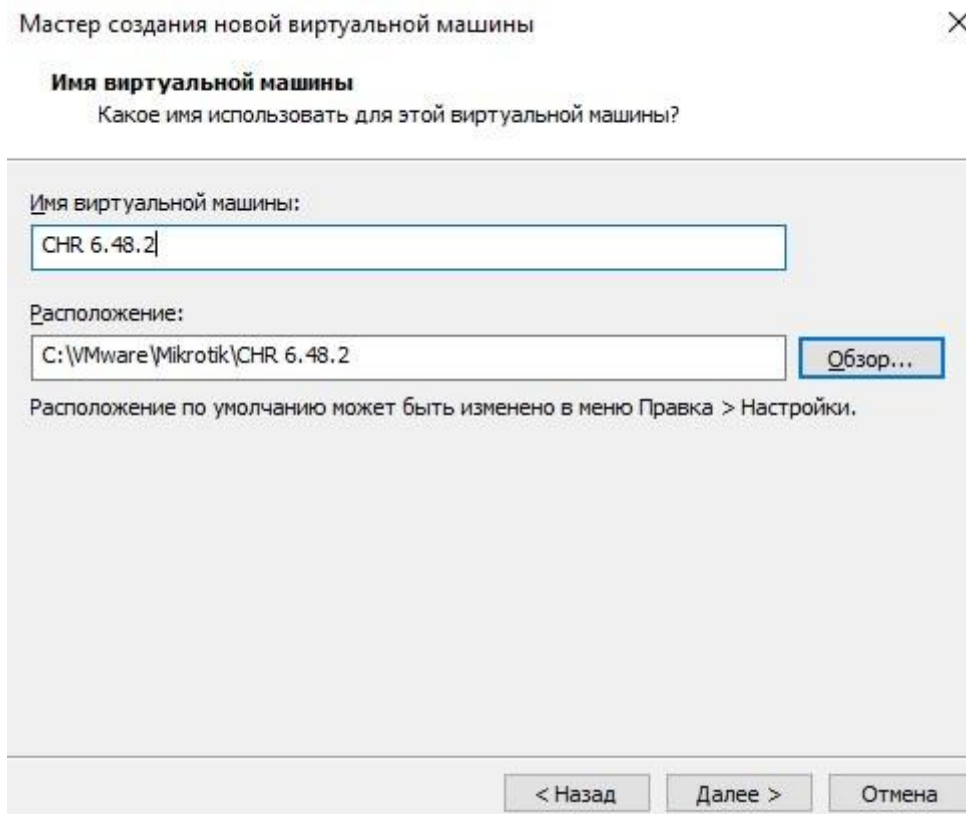


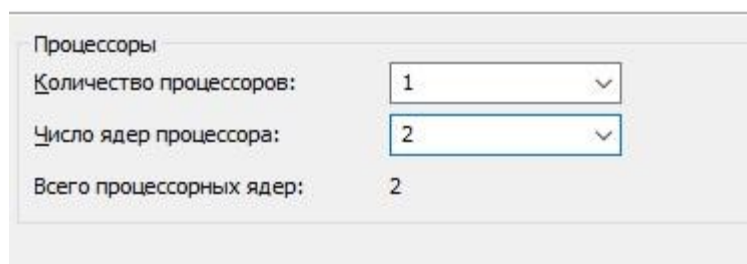
Рисунок 1.8 – Диалоговое окно создания новой VM

Mikrotik CHR не является ресурсоемкой ОС, но для избегания возможных зависаний во время работы выделим ей 2 ядра CPU.

Мастер создания новой виртуальной машины

Конфигурация процессора

Укажите количество процессоров для этой виртуальной машины



Процессоры	
Количество процессоров:	1
Число ядер процессора:	2
Всего процессорных ядер:	2

Рисунок 1.9 – Диалоговое окно создания новой VM

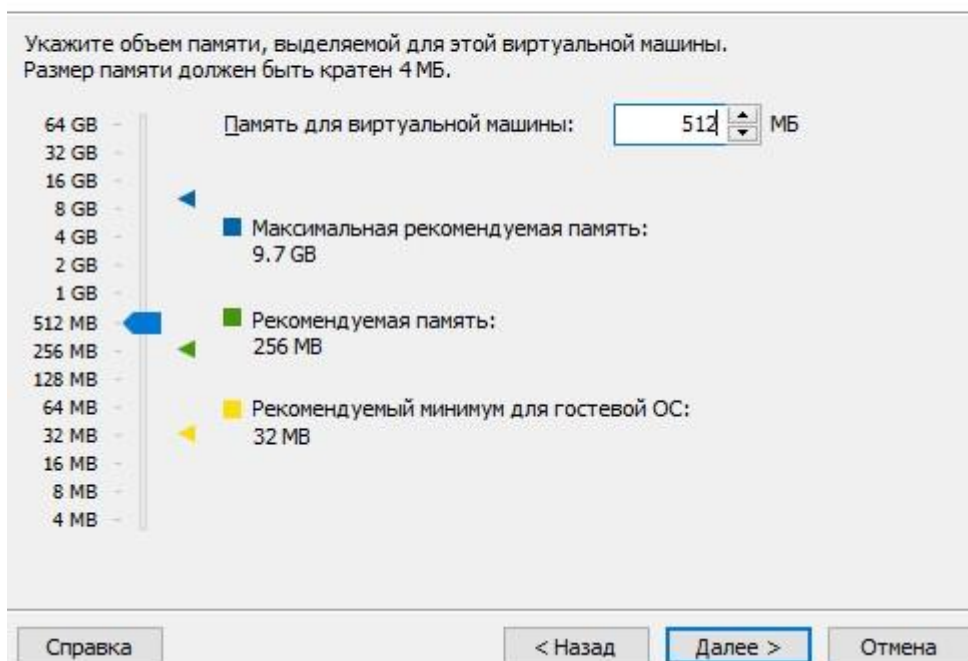
А также 512 оперативной памяти. Хотя и 256 было бы вполне достаточно. Множество устройств Mikrotik комплектуются микросхемами памяти от 64 до 256 Мбайт.

Мастер создания новой виртуальной машины



Память для виртуальной машины

Сколько памяти нужно выделить для этой виртуальной машины?



Укажите объем памяти, выделяемой для этой виртуальной машины.
Размер памяти должен быть кратен 4 МБ.

Память для виртуальной машины: 512 МБ

Максимальная рекомендуемая память: 9.7 GB

Рекомендуемая память: 256 MB

Рекомендуемый минимум для гостевой ОС: 32 MB

Справка < Назад **Далее >** Отмена

Рисунок 1.10 – Диалоговое окно создания новой VM

Далее требуется сконфигурировать сетевую карту устройства, так как в работе будет использоваться конфигурация устройств через графический и консольный интерфейсы, один из портов должен принадлежать множеству «сетевой мост». Так, устройство будет получать адрес из той же локальной сети, что и персональный компьютер. Для организации связи между двумя и более устройств необходимо использовать подсеть типа «Host Only» (сеть хоста). Дополнительные виртуальные подсети можно добавить через интерфейс «Edit – Virtual Networks». Ознакомиться с настройкой виртуальных сетей можно из официальной документации VMWare или сторонних новостных ресурсов, например: <https://web-profi.by/nastrojka-seti-vmware-workstation/>

Мастер создания новой виртуальной машины

Тип сети

Какой тип сети вы хотите добавить?

Сетевое подключение

- ☒ **Использовать сетевой мост**
Предоставление гостевой операционной системы прямого доступа к внешней сети Ethernet. Гостевая ОС должна иметь свой собственный IP-адрес внешней сети.
- ☐ **Использовать трансляцию сетевых адресов (NAT)**
Предоставление гостевой операционной системы доступ к подключению узла-компьютера или внешнего подключения по сети Ethernet с использованием IP-адреса узла.
- ☐ **Использовать только сеть узла**
Подключение к частной виртуальной сети на компьютере гостевой операционной системы.
- ☐ **Не использовать сетевое соединение**

Рисунок 1.11 – Диалоговое окно создания новой VM

Тип контроллера ввода-вывода оставляем по умолчанию.

Мастер создания новой виртуальной машины

Выбор типов контроллеров ввода/вывода

Какой тип SCSI-контроллера нужно использовать?

Типы контроллеров ввода-вывода

Контроллер SCSI:

- ☐ BusLogic (Не доступно для 64-разрядных гостевых ОС)
- ☒ **LSI Logic** (рекомендуется)
- ☐ LSI Logic SAS
- ☐ Паравиртуализированный SCSI

Рисунок 1.12 – Диалоговое окно создания новой VM

Тип жёсткого диска меняем с IDE на SATA.

Мастер создания новой виртуальной машины

Выбор типа диска

Какой диск вы хотите создать?

Тип виртуального диска

- ☐ IDE (рекомендуется)
- ☐ SCSI
- ☒ **SATA**
- ☐ NVMe

Рисунок 1.13 – Диалоговое окно создания новой VM

Выбираем «использовать существующих виртуальный диск».

Мастер создания новой виртуальной машины



Выбор диска

Какой диск вы хотите использовать?

Диск

☐ Создать новый виртуальный диск

Виртуальный диск состоит из одного или нескольких файлов в файловой системе узла, которые будут выглядеть как единый жесткий диск для гостевой операционной системы. Виртуальные диски можно легко копировать или перемещать на одном и том же узле или между узлами.

☒ Использовать существующий виртуальный диск

Выберите этот параметр для повторного использования ранее настроенного диска.

☐ Использовать и физический диск (для опытных пользователей)

Выберите этот параметр, чтобы предоставить виртуальному компьютеру прямой доступ к локальному жесткому диску. Требуется права администратора.

Справка < Назад **Далее >** Отмена

Рисунок 1.14 – Диалоговое окно создания новой VM

В следующем окне мастера указываем путь до него.

Мастер создания новой виртуальной машины



Выбор существующего диска

Какие ранее настроенные диски использовать?

Существующий файл диска

C:\VMware\Mikrotik\CHR 6.48.2\chr-6.48.2.vmdk **Обзор...**

Рисунок 1.15 – Диалоговое окно создания новой VM

Сохраняем существующий формат.

VMware Workstation



Преобразовать существующий виртуальный диск в новый формат?

Выбранный виртуальный диск может быть преобразован в новый формат, поддерживаемый этой виртуальной машиной Workstation 15.x. Тем не менее, после преобразования виртуальный диск не будет работать со устаревшими виртуальными машинами.

Сохранить существующий формат Преобразовать Отмена

Рисунок 1.16 – Диалоговое окно создания новой VM

Проверяем конфигурацию и жмем готово.

Все готово для создания виртуальной машины

Нажмите кнопку Готово, чтобы создать виртуальную машину. Затем можно начать установку Other 64-bit.

Виртуальная машина будет создана со следующими параметрами:

Имя:	CHR 6.48.2
Расположение:	C:\VMware\Mikrotik\CHR 6.48.2
Версия:	Workstation 15.x
Операционная ...	Other 64-bit
Жесткий диск:	Существующий диск C:\VMware\Mikrotik\CHR 6.48...
Память:	512 МБ
Сетевой адапт...	Мост (автоматически)
Другие устрой...	Ядер ЦП: 2, CD/DVD, Звуковая карта

Настройка оборудования...

< Назад

Готово

Отмена

Рисунок 1.17 – Диалоговое окно создания новой VM

Запускаем машину.

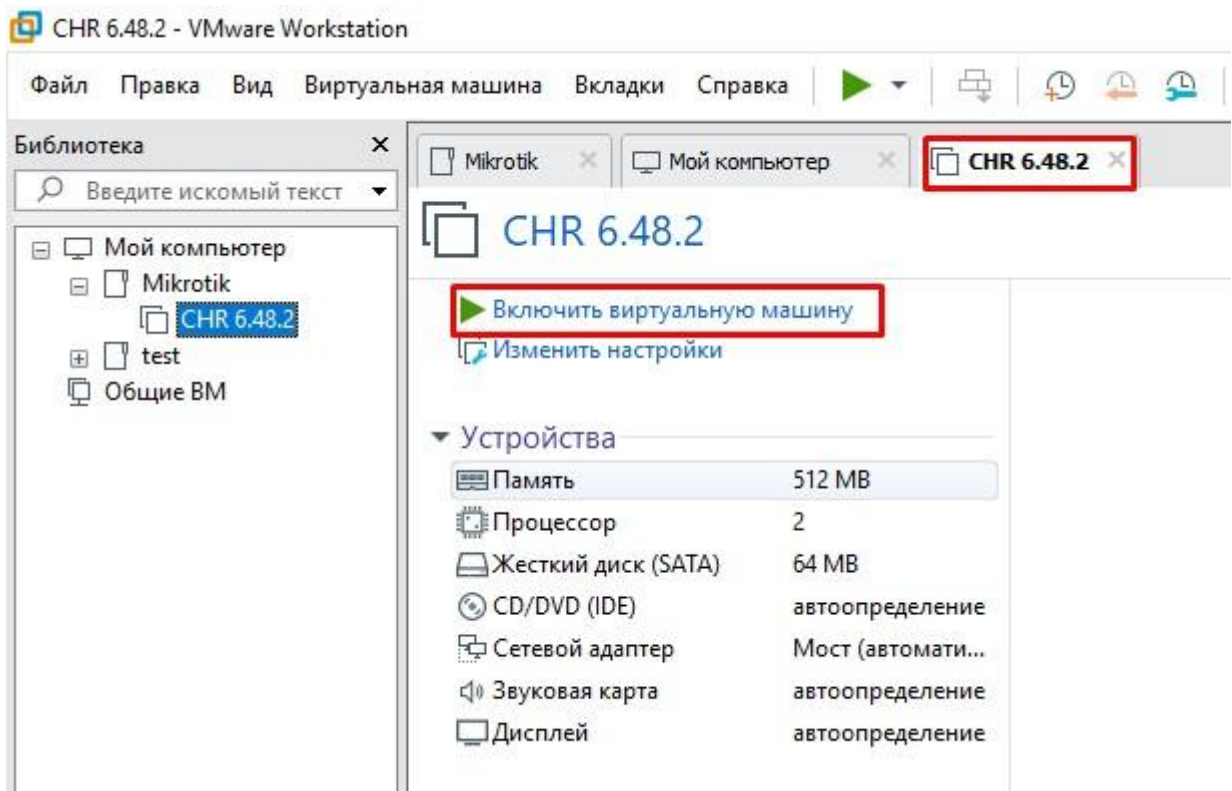


Рисунок 1.18 – Запуск виртуальной машины

1.4 Подключение к CHR на VMWare

По умолчанию в CHR установлено, что на первом интерфейсе всегда включен dhcp-client при первом запуске. Посмотрим какой адрес получил RouterOS.

```
CHR 6.48.2

MMM MMMM MMM III KKK KKK RRRRRR 000000 TTT III KKK KKK
MMM MM MMM III KKKKK RRR RRR 000 000 TTT III KKKKK
MMM MMM III KKK KKK RRRRRR 000 000 TTT III KKK KKK
MMM MMM III KKK KKK RRR RRR 000000 TTT III KKK KKK

MikroTik RouterOS 6.48.2 (c) 1999-2021 http://www.mikrotik.com/

Do you want to see the software license? [Y/n]: n
[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level

[admin@MikroTik] > ip dhcp-client print
Flags: X - disabled, I - invalid, D - dynamic
# INTERFACE USE ADD-DEFAULT-ROUTE STATUS ADDRESS
0 ether1 yes yes bound 192.168.10.12
line 2 of 2>
```

Рисунок 1.19 – Проверка сетевого адреса устройства MikroTik CHR

Устройства MikroTik управляются через консоль, веб-интерфейс или специализированное ПО Winbox, доступное для скачивания на официальном сайте MikroTik. Подключимся через Winbox и взглянем на Resources (По умолчанию логин и пароль MikroTik admin:пароль пустой). Для установки пароля можно воспользоваться командой /user edit admin password

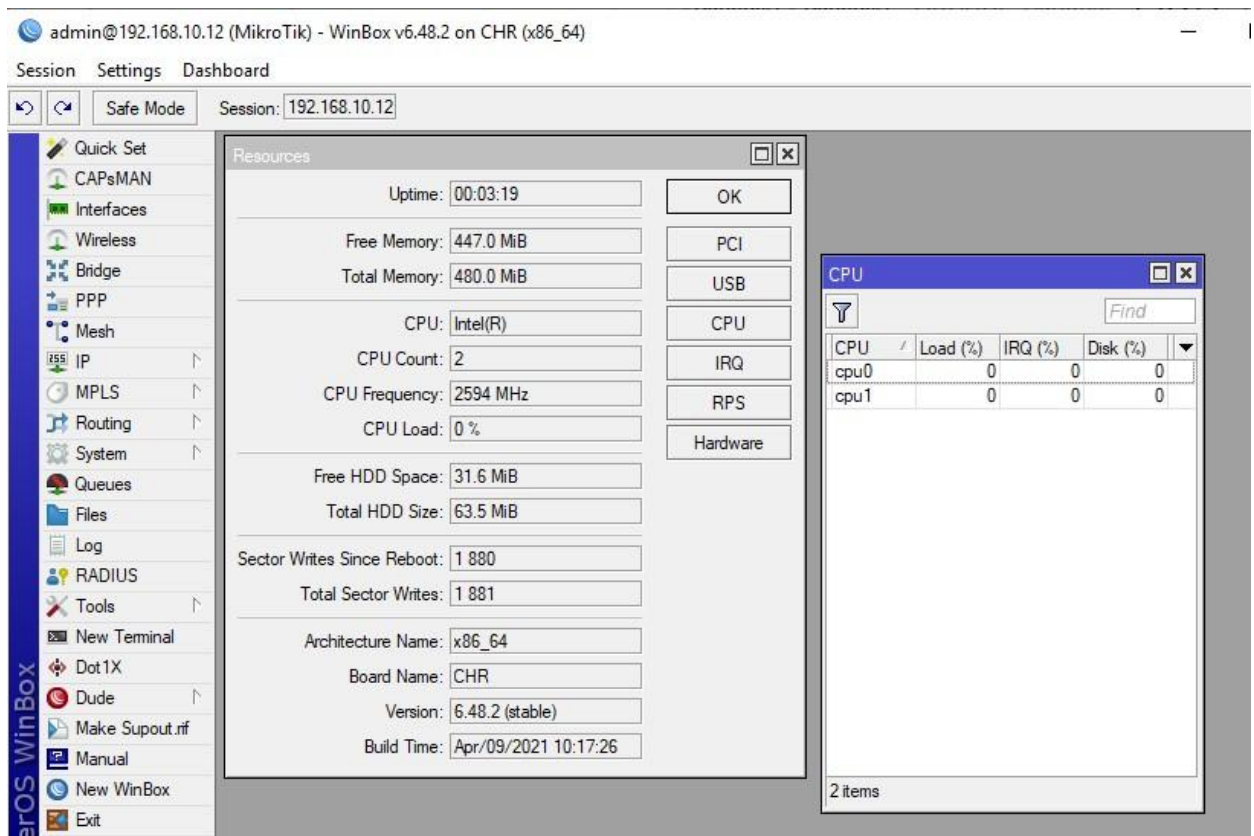


Рисунок 1.20 – Интерфейс ПО Winbox

Ядра на месте, ОЗУ тоже. Так же видно дату запуска и многое другое. Настройка Микротик CHR на VMWare не сложный процесс. Но немного длиннее, т.к. мастер предлагает множество вариаций по типам подключений жёсткого диска. В целом вы можете экспортировать данную VM и средством импорта ее размножить.

2. Настройка SSTP Сервера и клиента

Далее рассмотрим как настроить SSTP Server на MikroTik. Расшифровывается аббревиатура как Secure Socket Tunneling Protocol – PPP туннель аутентифицирует через TLS канал. Использует TCP порт 443 и фактически проходит через все сетевые экраны и прокси сервера. Впервые был представлен в Windows Vista SP1. С того момента прошло много времени, но до сих пор используется ввиду наличия неоспоримых преимуществ:

- Безопасный, используются алгоритмы AES;
- Полностью поддерживается MS Windows.

Из минусов:

- работает на одном ядре;
- уязвим перед некоторыми атаками MITM.

2.1 Схема сети

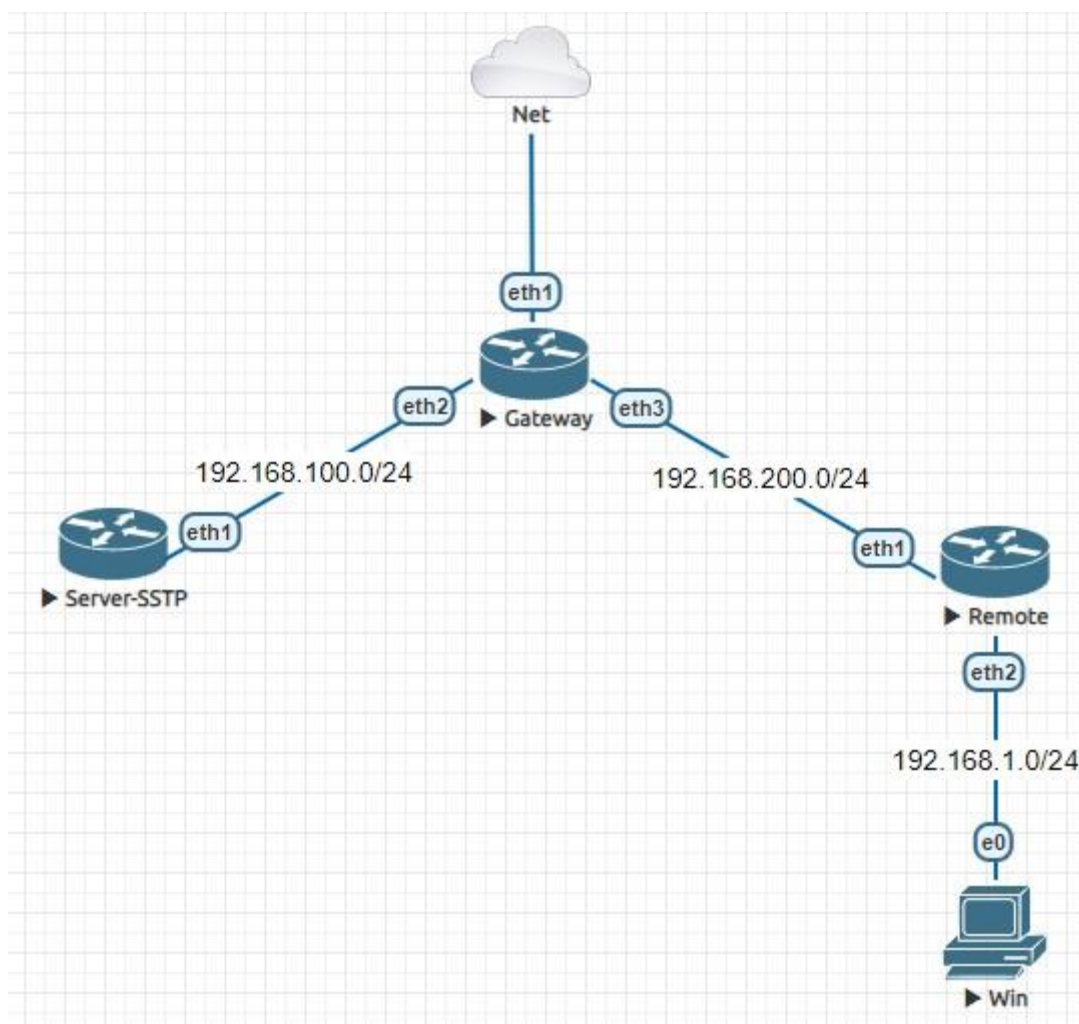


Рисунок 2.1 – Схема моделируемой сети

- Сервер SSTP имеет адрес 192.168.100.2;
- Клиентский ПК получает из пула 192.168.1.0/24;
- Маршрутизируемая сеть между удаленными площадками.

2.2 Настройка сервера SSTP

Конфигурация устройства проста. Имеем RouterBoard с настроенным выходом в интернет. Подключение будет происходить по сертификату, в котором вместо

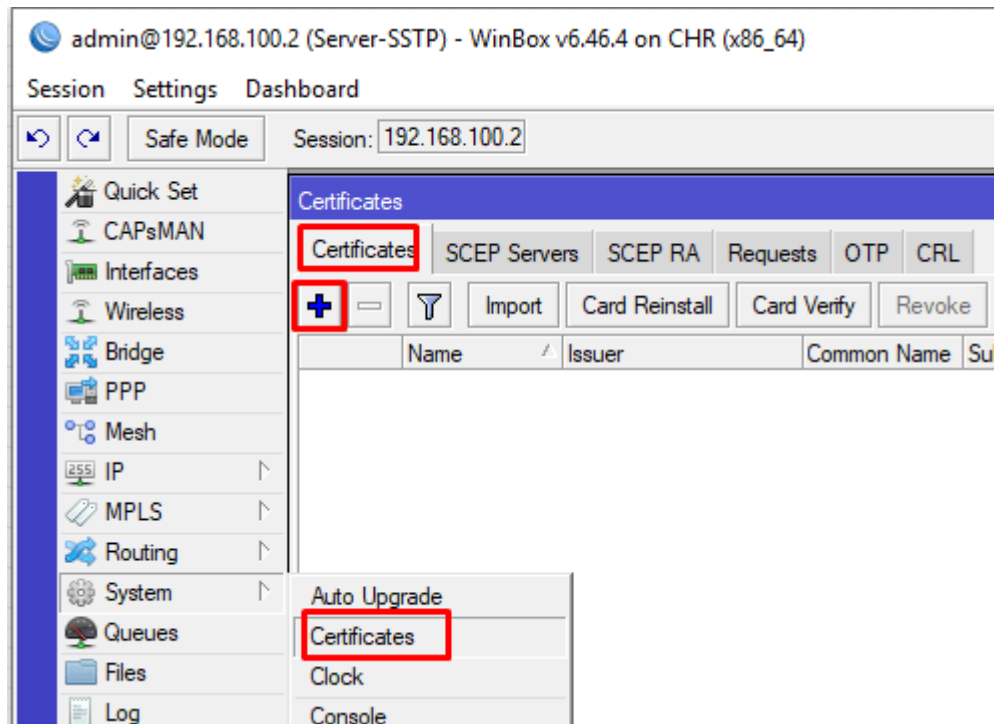


Рисунок 2.2 – Создание сертификата

В поле Name указываем понятное имя, отображаемое в списке;

- Country – двухбуквенное значение;
- State, Locality, Organization, Unit – по своему усмотрению;
- Common Name – самое важное, уникальное имя.

Если у вас есть доменное имя vpn.test.ru, то вписываете его сюда. Если же его нет, но есть публичный статический адрес, то пишете его. Представим, что наш адрес такой.

Вы так же можете указать длину ключа и срок действия.

The 'New Certificate' dialog box is shown with the 'General' tab selected. It contains the following fields:

- Name: CA
- Issuer: (empty)
- Country: RU
- State: MSC
- Locality: MSC
- Organization: Remote
- Unit: Access
- Common Name: 192.168.100.2
- Subject Alt. Name: (empty)
- Key Type: (empty)
- Key Size: 2048
- Days Valid: 365

On the right side, there is a vertical stack of buttons: OK, Cancel, Apply, Copy, Remove, Sign, Sign via SCEP, Create Cert. Request, Import, Card Reinstall, Card Verify, Export, and Revoke.

Рисунок 2.3 – Настройка сертификата

Далее переходим в Key Usage. Снимаем галки со всего, оставляя только на `crf sign` и `key cert. sign`.

The 'New Certificate' dialog box is shown with the 'Key Usage' tab selected. It displays a list of key usage options with checkboxes:

- ☐ digital signature
- ☐ key encipherment
- ☐ key agreement
- ☒ **crf sign**
- ☐ decipher only
- ☐ server gated crypto
- ☐ timestamp
- ☐ ipsec tunnel
- ☐ email protect
- ☐ tls client
- ☐ content commitment
- ☐ data encipherment
- ☒ **key cert. sign**
- ☐ encipher only
- ☐ dvcs
- ☐ ocsp sign
- ☐ ipsec user
- ☐ ipsec end system
- ☐ code sign
- ☐ tls server

The checkboxes for 'crf sign' and 'key cert. sign' are highlighted with red boxes.

Рисунок 2.4 – Настройка сертификата

Жмем Apply и Sign. В новом открывшемся окне подписания, запускаем процесс подписи кнопкой Start.

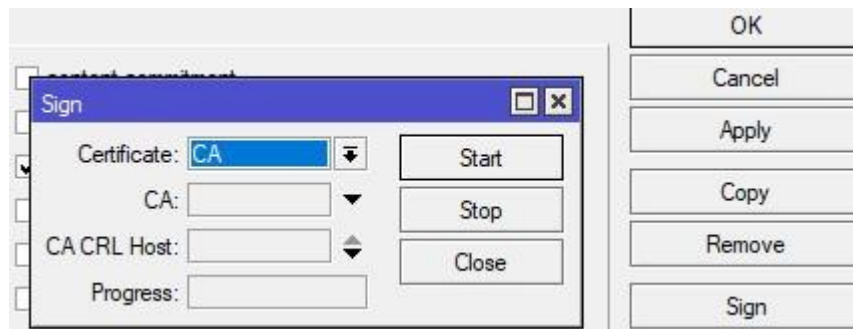


Рисунок 2.5 – Настройка сертификата

По завершении увидим в Progress состояние done и аббревиатуру KAT возле CA.



Рисунок 2.6 – Проверка сертификата

Далее создаем сертификат самого сервера SSTP, который будет указан в качестве основного на интерфейсе. Жмем плюс и заполняем все поля аналогично предыдущему, за исключением понятного имени.

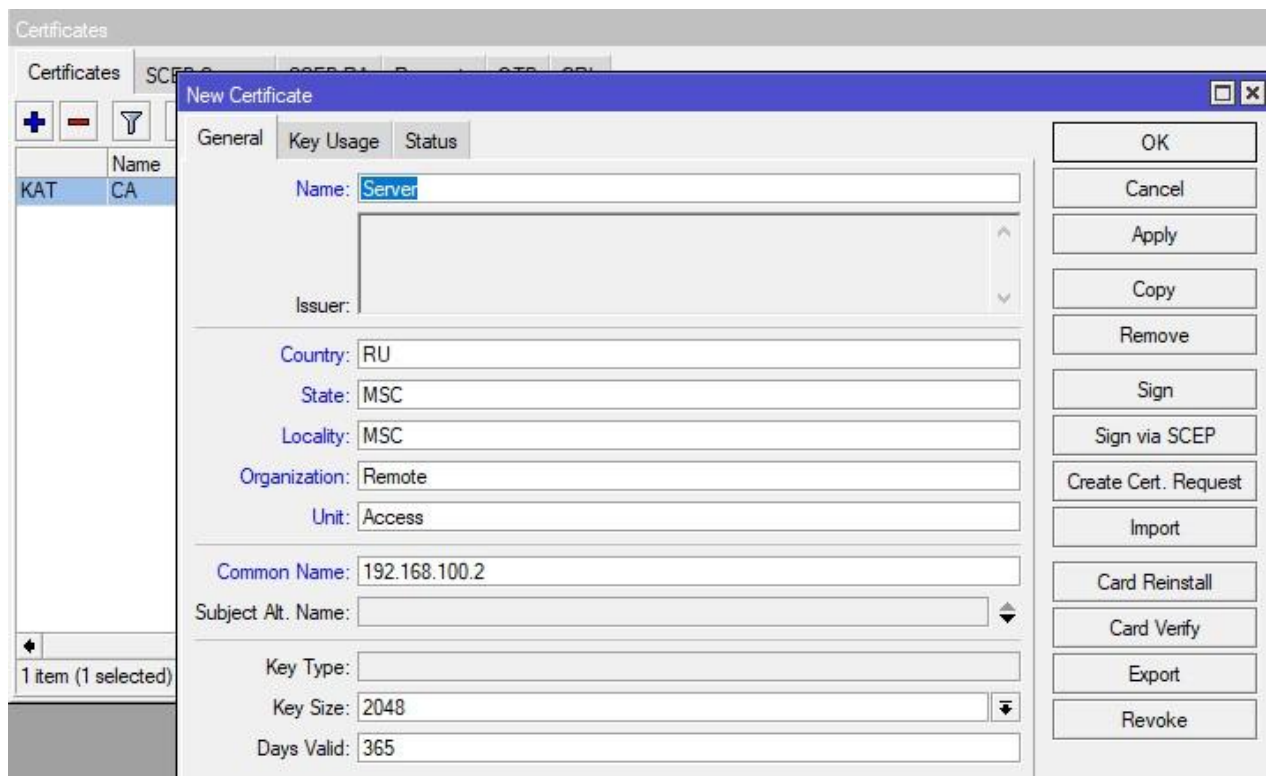


Рисунок 2.7 – Настройка сертификата

На вкладке Key Usage добавляем галочки tls client и tls server.



Рисунок 2.8 – Настройка сертификата

Жмем Apply и Sign. В открывшемся окне подписи в поле CA выбираем корневой сертификат и запускаем процесс.

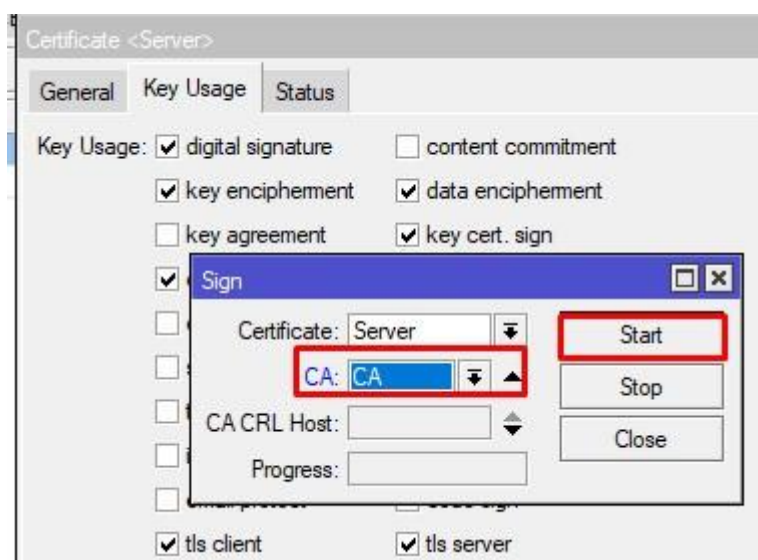


Рисунок 2.9 – Настройка сертификата

Проверим.

Certificates								
Certificates SCEP Servers SCEP RA Requests OTP CRL								
+ - Filter Import Card Reinstall Card Verify Revoke Settings								
	Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL
KAT	CA		192.168.100.2		2048	365	yes	
KA	Server		192.168.100.2		2048	365	no	

Рисунок 2.10 – Листинг сертификатов

Далее создадим профиль подключения для клиентов. PPP – Profiles. Указываем понятное имя профиля;

- адрес в туннеле;

- разрешаем TCP MSS;
- запрещаем UPnP.

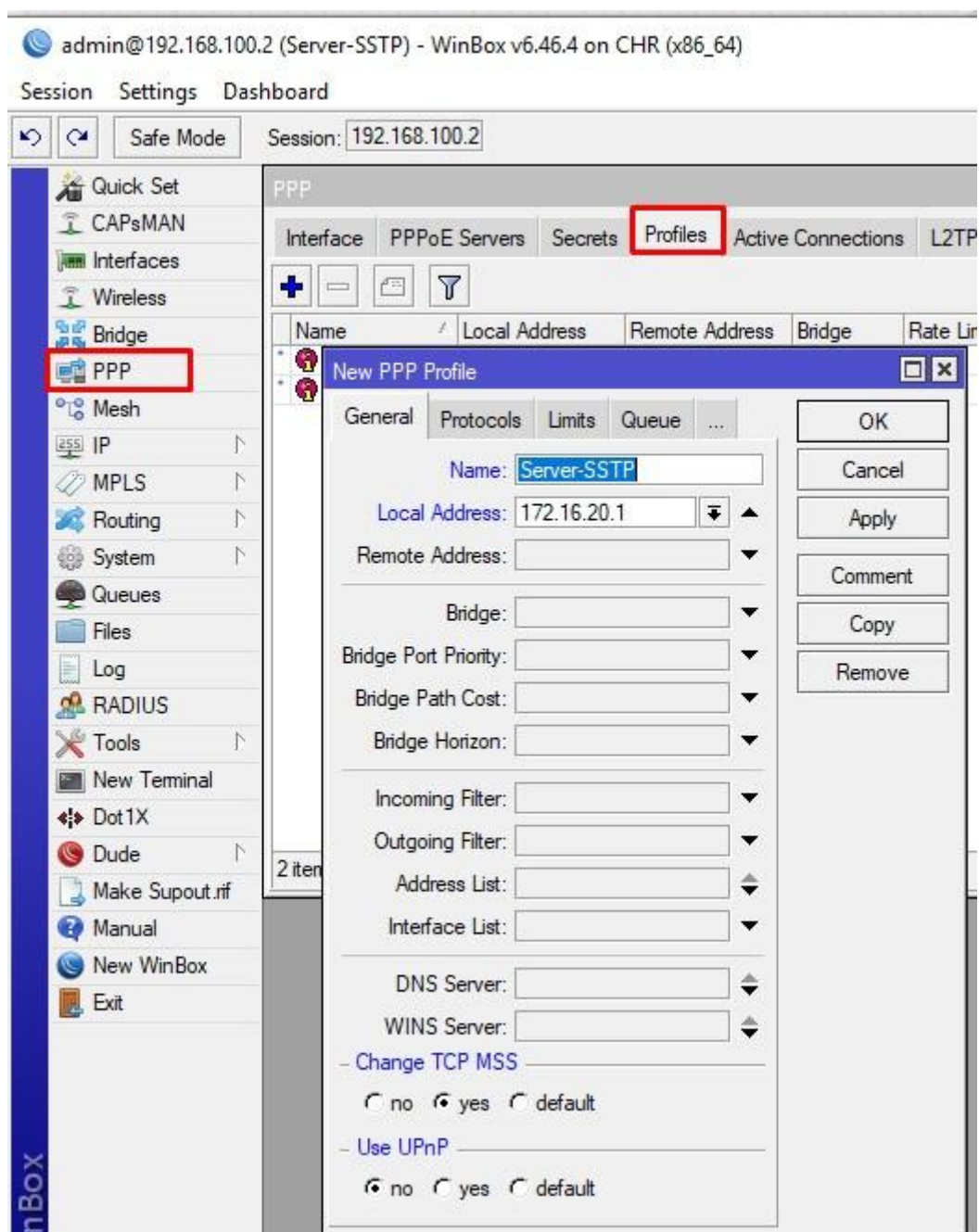


Рисунок 2.11 – Создание профайлов пользователей

В Protocols:

- Use MPLS – запретить;
- Use Compression – разрешить;
- Use Encryption – разрешить;

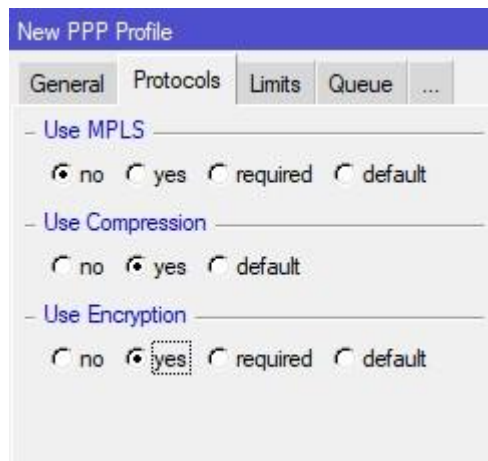


Рисунок 2.12 – Создание профайлов пользователей

В Limits выставляем Only One в no.

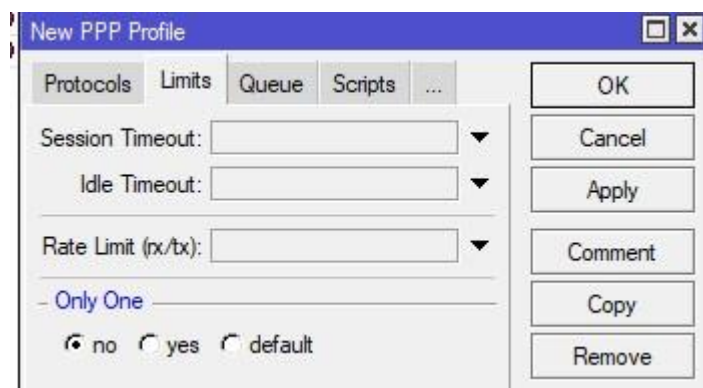


Рисунок 2.13 – Создание профайлов пользователей

Создадим пользователя в Secrets.

- Name – имя пользователя, регистр имеет значение;
- Password – пароль;
- Service – SSTP;
- Profile – созданный выше;
- Remote Address – адрес в туннеле.

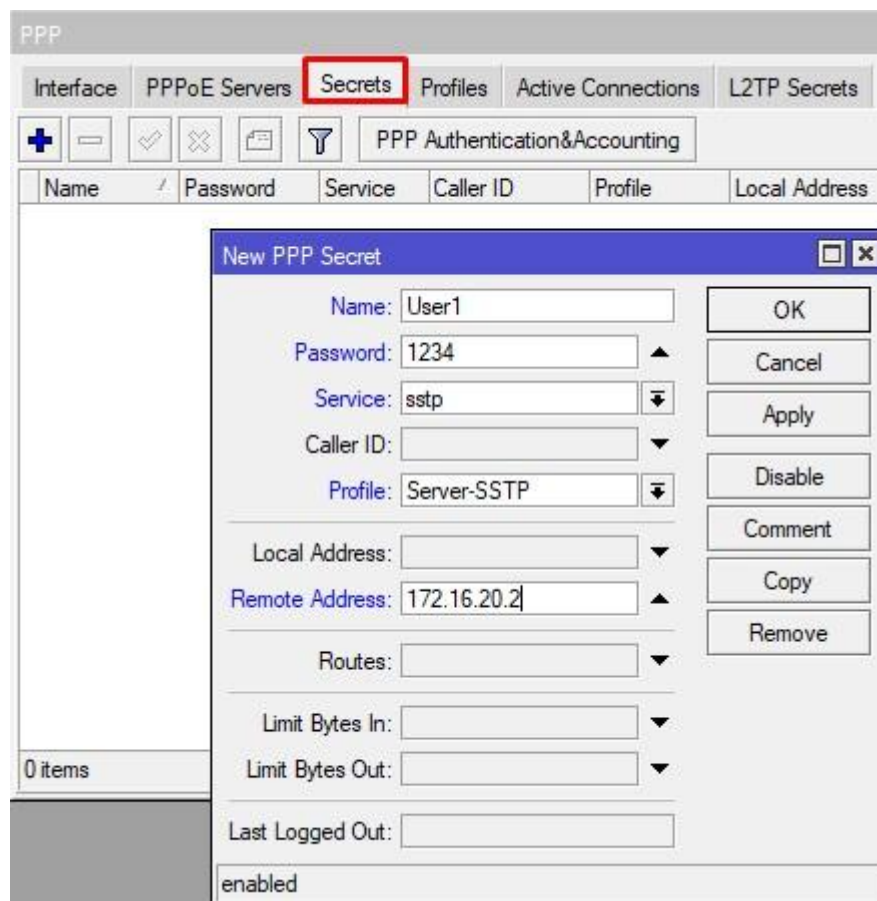


Рисунок 2.14 – Создание профайлов пользователей

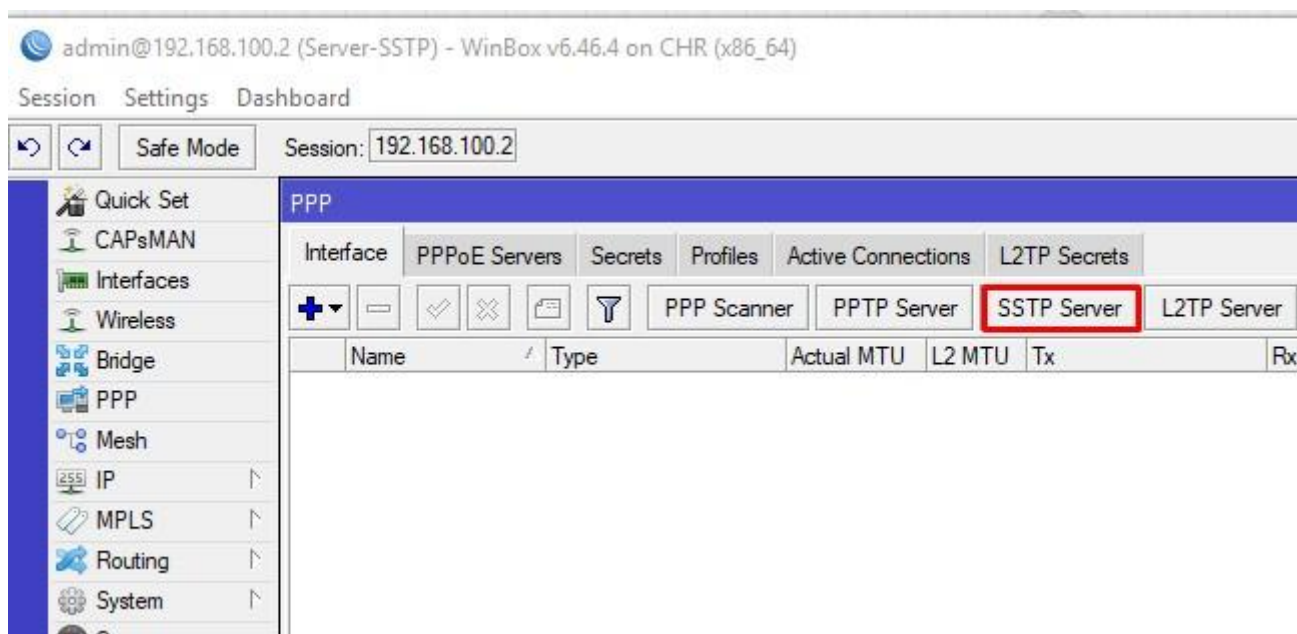


Рисунок 2.15 – Конфигурация SSTP сервера

Открыв ее, указываем следующие значения:

- Enable – ставим галочку;
- Default Profile – ранее созданный;
- Authentication – mschapv2;
- Certificate – Server;

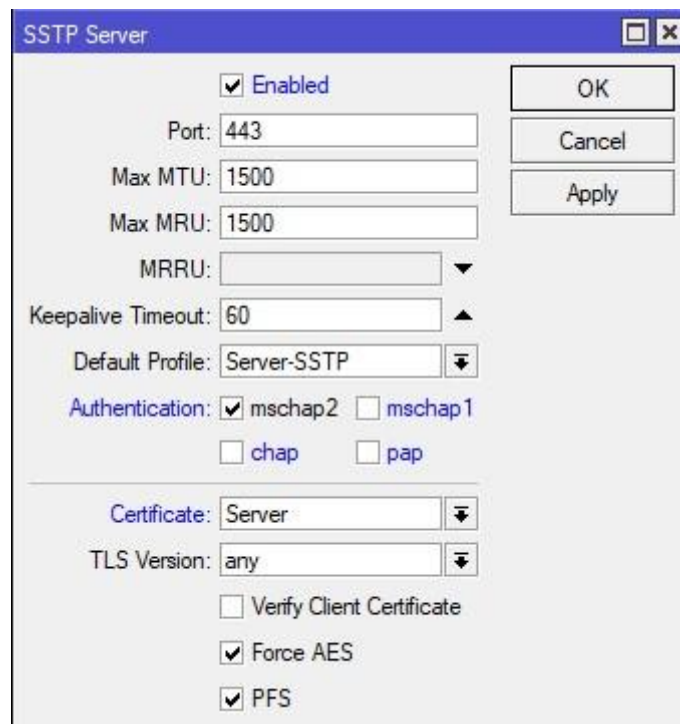


Рисунок 2.16 – Конфигурация SSTP сервера

Если безопасность соединения важна, то можно выставить TLS Version в only 1.2. Двигаемся дальше к фаерволу. Просто одно правило. Разрешить входящий трафик на 443 порт – все.

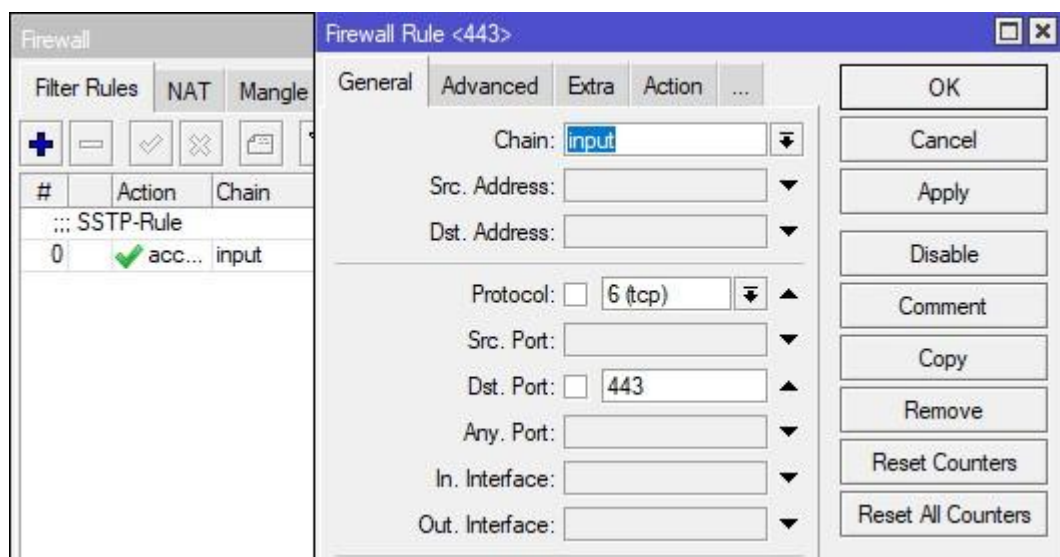


Рисунок 2.17 – Конфигурация сетевого экрана

2.3 Настройка SSTP клиента на Микротик

Для дальнейшей конфигурации нам нужен сертификат центра сертификации добавить в доверенные компьютера. Иначе начнутся проблемы со списком отзывов. Конечно, таких проблем не будет при использовании используя коммерческих сертификатов. Сертификат для начала нужно выгрузить. Открываем System – Certificates, выбираем CA и жмем Export.

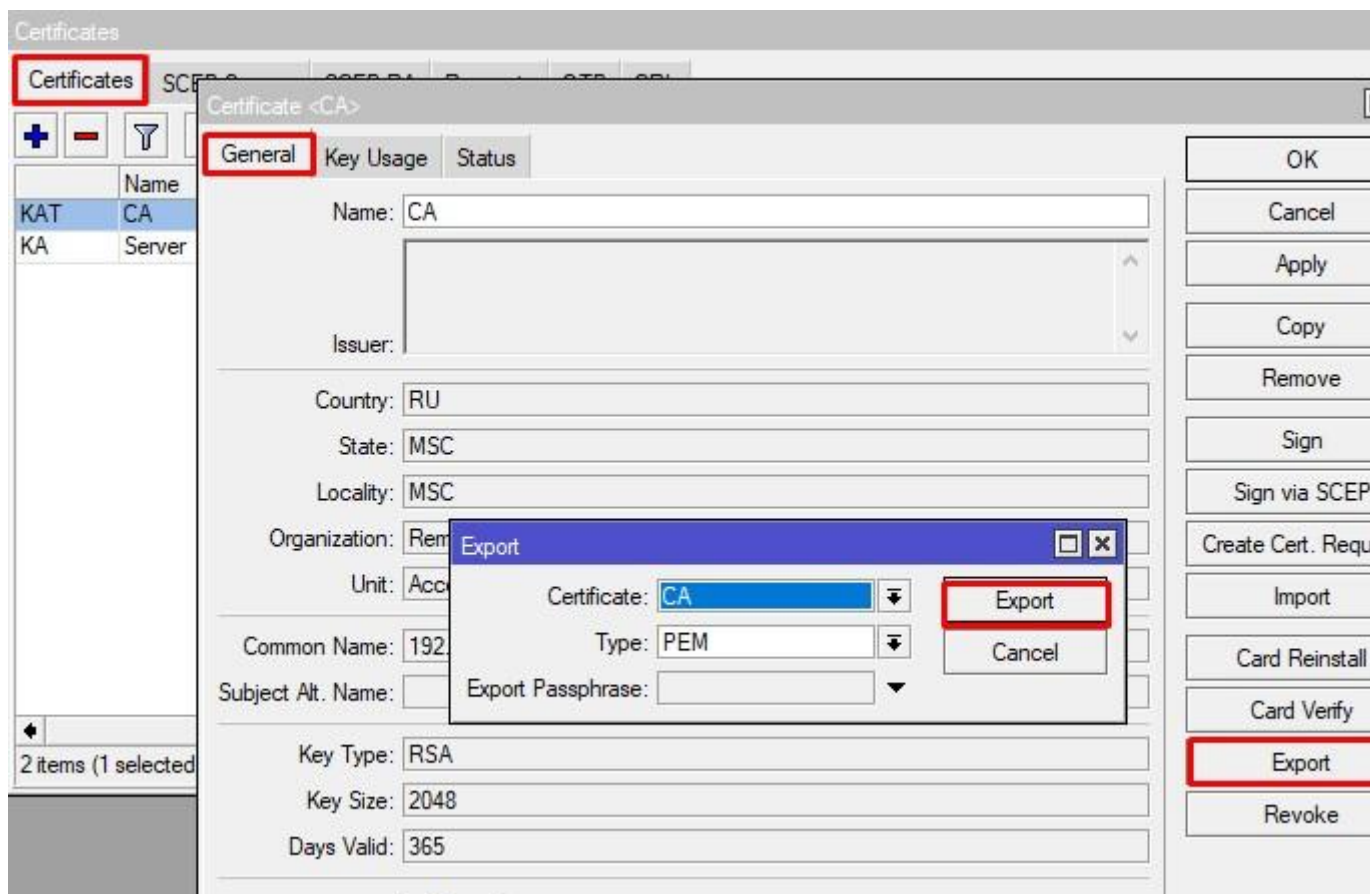


Рисунок 2.18 – Экспорт сертификата

В Files должен появиться экспорт. Передаем его любым удобным способом на клиентскую машину.

Далее вы можете вручную его добавить в доверенные ПК, но также можно использовать скрипт. Сохраняем в формате .bat
Создаем на рабочем столе папу CA, копируем туда CA.crt и запускаем из-под администратора bat-скрипт.

```
cd «%UserProfile%\Desktop\CA»  
certutil -addstore «Root» CA.crt
```

Проверяем что все хорошо (Win+R -> certmgr, это действие откроет окно на следующем рисунке).

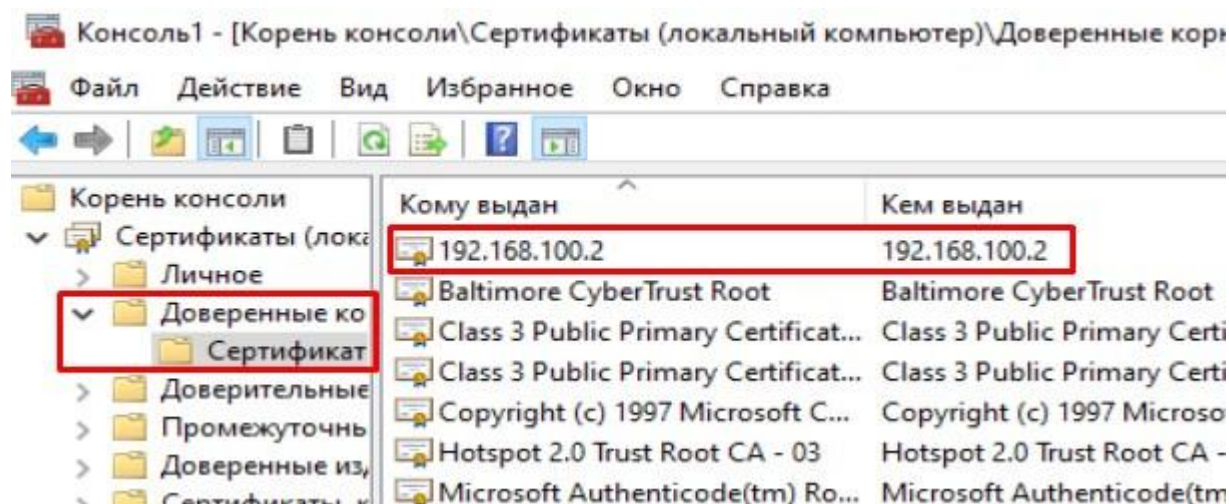


Рисунок 2.19 – Интерфейс менеджера сертификатов Windows

Далее переходим в Центра управления сетями и общим доступом – Создание и настройка нового подключения или сети.

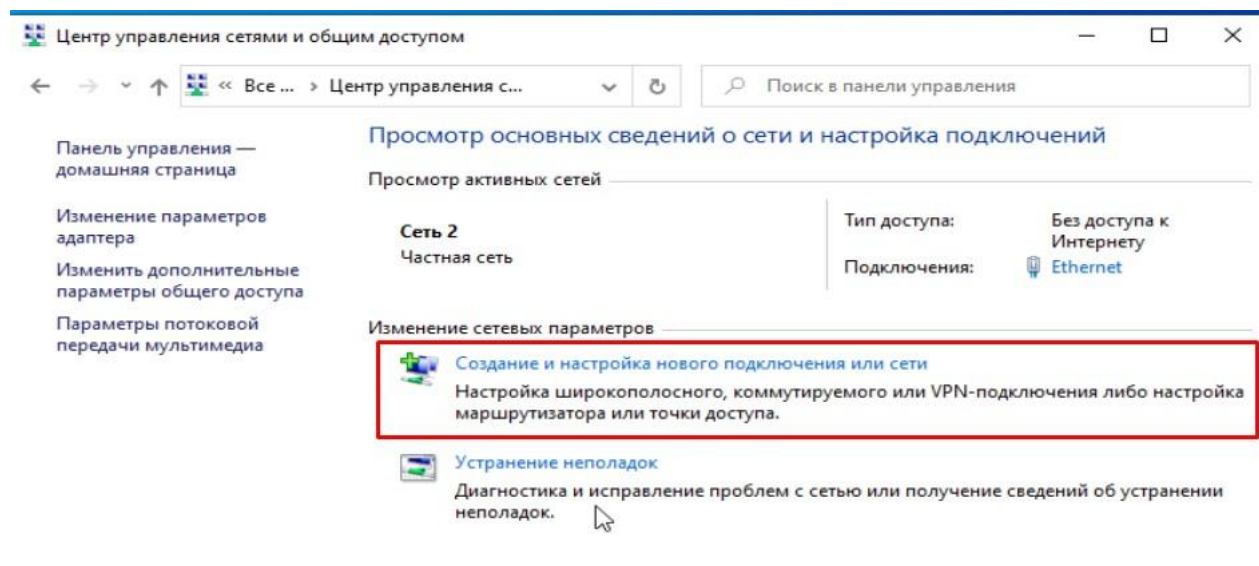


Рисунок 2.20 – Конфигурация SSTP клиента

Подключение к рабочему месту.

Выберите вариант подключения

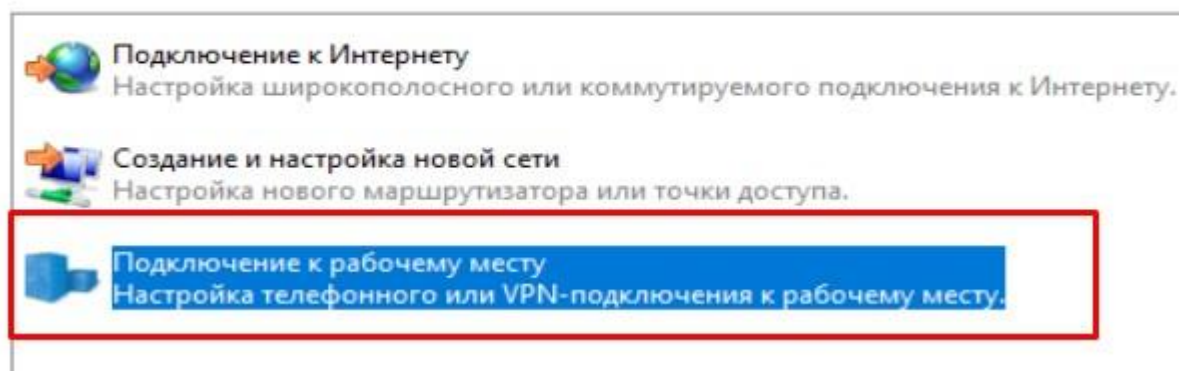


Рисунок 2.21 – Конфигурация SSTP клиента

← Подключение к рабочему месту

Как вы хотите выполнить подключение?

→ **Использовать мое подключение к Интернету (VPN)**
Подключение через Интернет с помощью виртуальной частной сети (VPN).



→ **Использовать прямой набор номера**
Прямое подключение к телефонному номеру без выхода в Интернет.



Рисунок 2.22 – Конфигурация SSTP клиента

← Подключение к рабочему месту

Введите адрес в Интернете

Этот адрес можно получить у сетевого администратора.

Адрес в Интернете:

192.168.100.2

Имя объекта назначения:

SSTP

☐ Использовать смарт-карту

☒ Запомнить учетные данные



☐ Разрешить использовать это подключение другим пользователям

Этот параметр позволяет любому пользователю, имеющему доступ к этому компьютеру, использовать данное подключение.

Рисунок 2.23 – Конфигурация SSTP клиента

Переходим в «Изменение параметров адаптера» и открываем свойства VPN интерфейса. На вкладке «Тип VPN» переключить с автоматически на SSTP, Проверку подлинности переключить на Microsoft CHAP версии 2.

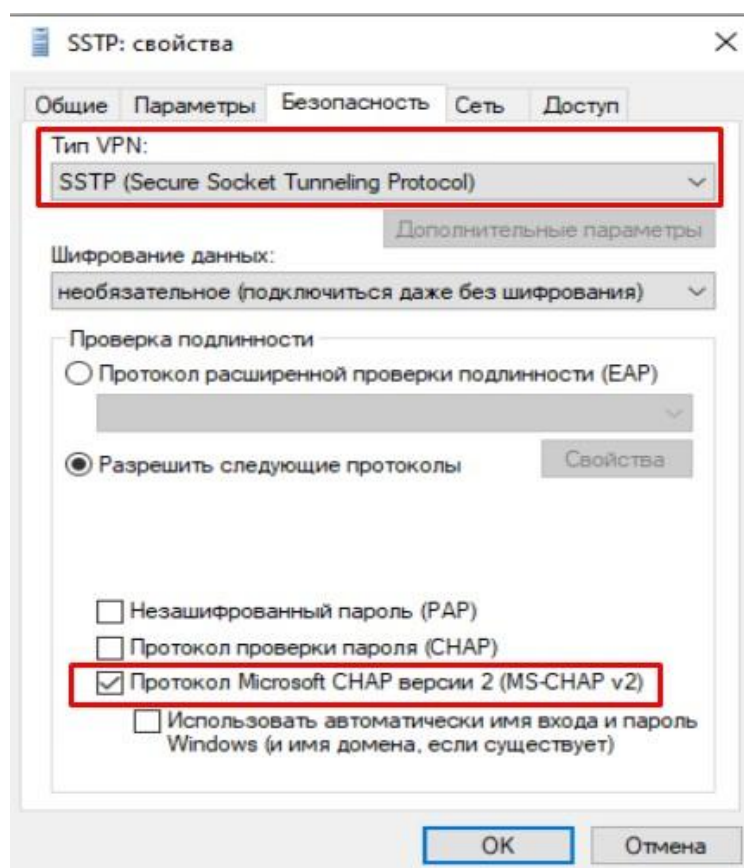


Рисунок 2.24 – Конфигурация SSTP клиента

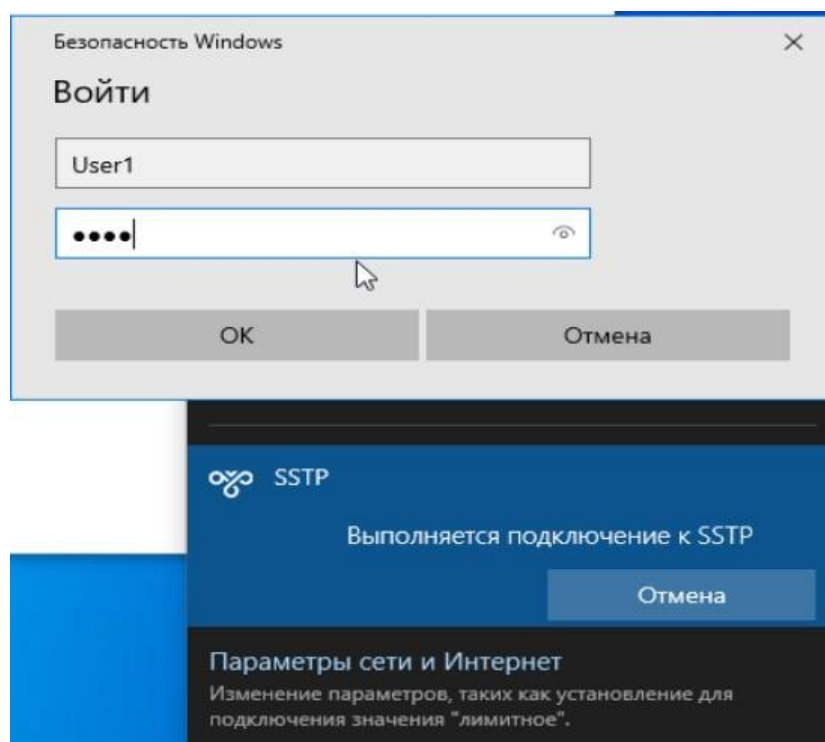


Рисунок 2.25 – Установление SSTP туннеля

Возможные ошибки:

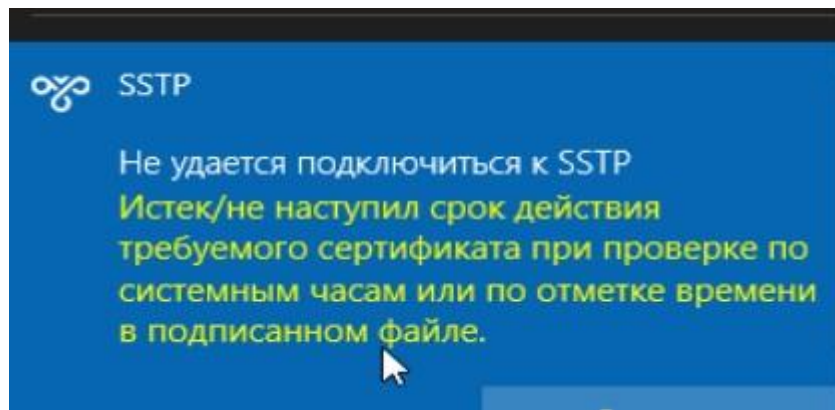


Рисунок Рисунок 2.26 – Ошибка SSTP

Это связано со временем. Т.к. в виртуальных машинах оно идет по-другому. Открыв свойства сертификата, можно заметить, что срок, с которого действителен сертификат еще не наступил. Исправив время на правильное, все заработало. Проверка подключения на клиенте и сервере:

