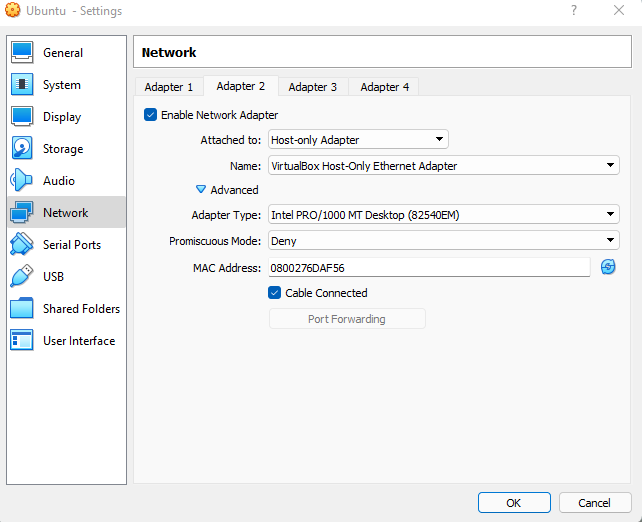
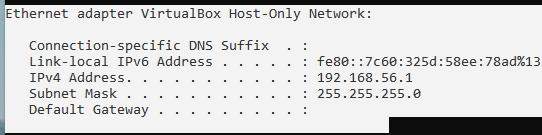
**SSH** (Secure Shell — “безопасная оболочка”) — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой, туннелирование TCP-соединений (например, для передачи файлов), и позволяет осуществлять управлению OS через CLI. Шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

SSH-сервер обычно прослушивает соединения на TCP-порту 22.

1. **Создаем виртуальную машину, к которой будем подключаться. Добавляем ей адаптер Host-Only**



1. **Настраиваем адаптер (назначаем ему IP адрес, маску сети, широковещательный адрес, а так же поднимаем интерфейс)**
   1. *Узнаем какой IP адрес у сети нашего адаптера. На хост машине выполняем команду ipconfig и смотрим*



* 1. *Смотрим какие у нас есть интерфейсы, и какие из них поднятые*

sudo ip link show

sudo ip link show up

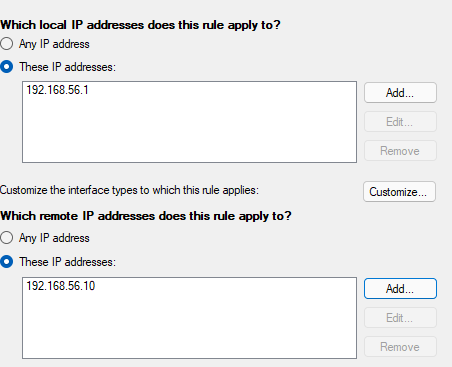
* 1. *Поднимаем добавленный интерфейс, а после настраиваем его*

sudo ip link set dev enp0s8 up

sudo ip a add 192.168.56.10/24 broadcast 192.168.56.255 dev enp0s8

1. **Разрешаем подключение в firewall на хосте, что бы VM могла иметь доступ к хосту**

Добавляем Inbound Rule на все программы и порты, что IP адрес нашей виртуалки сможет иметь доступ



1. **Устанавливаем на VM ssh сервер + клиент**

sudo apt-get install openssh-server openssh-client

*На centOS используется:*

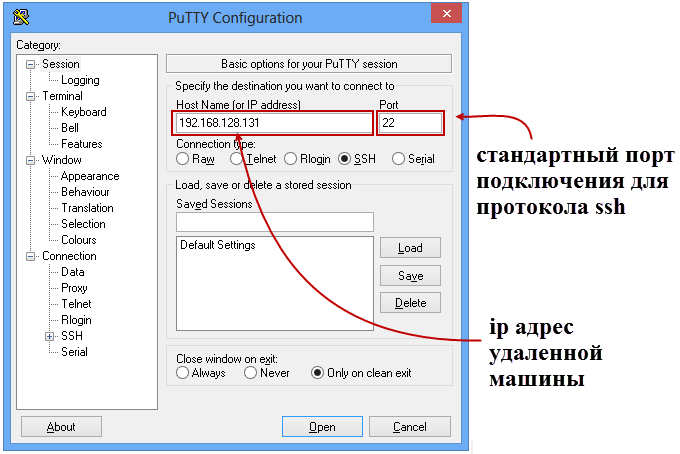
yum –y install openssh-server openssh-client

1. **Подключаемся к серверу через PuTTY**

[PuTTY](http://www.chiark.greenend.org.uk/~sgtatham/putty/) - cвободно распростроняемый клиент для протокола удаленного доступа SSH. Изначально разрабатывался для Microsoft Windows, однако позднее портирован на Unix.

Вообще список клиентов достаточно велик и для Linux, и для Windows, и не ограничивается одним Putty.

Что бы подключиться к серверу, нужно что бы он был в 1 сети, мы знали его IP адрес и пароль



**Копирование файлов через SSH**

**SCP** — протокол RCP копирования файлов, использующий в качестве транспорта SSH.

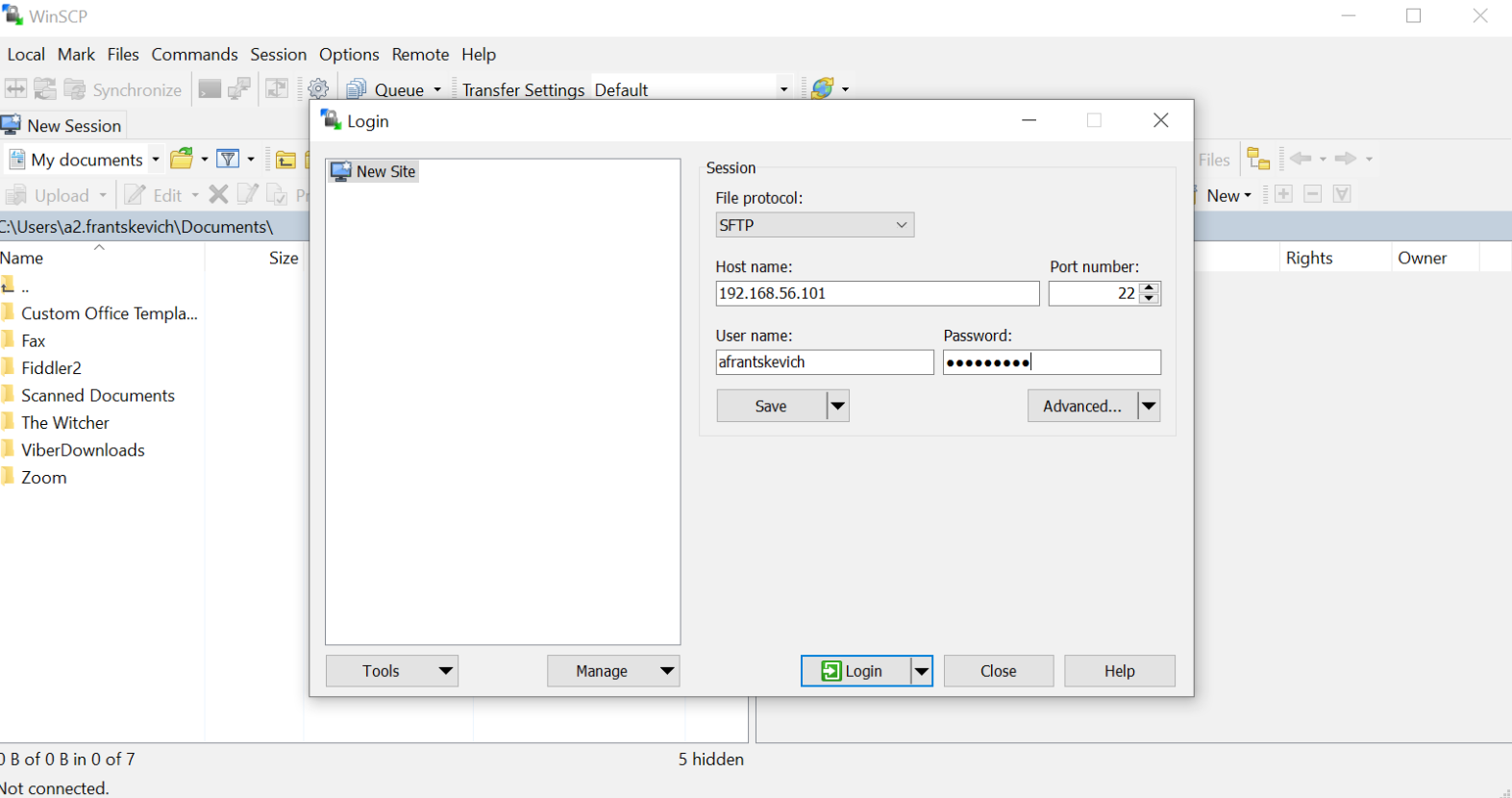
Клиент для OS Windows: [winSCP](http://winscp.net/eng/download.php).

**Windows – через программу:**

1. Качаем winscp <https://winscp.net/eng/download.php>

2. Устанавливаем > открываем

3. Подключаемся к удаленному компьютеру (host/user/password)



4. Находим нужный файл с логами, копируем на свой ПК > вносим изменения > сохраняем

**Windows – через cmd**

**scp** откуда\_копируем куда\_копируем – копирует файл

scp artyom@artyom-VirtualBox:/home/artyom/Desktop/test.txt C:\Users\artiv\Desktop - скопировать файл с Linux на хост Windows

**scp -r** откуда\_копируем куда\_копируем - скопировать рекурсивно (папку со всем содержимым)

### 1. Настройка подключения к удаленной машине по SSH

***Linux***:

1. Для подключения по SSH нам необходимо знать такие данные:

• ip адрес сервера, к которому мы собираемся подключится;

• порт, на котором ожидает подключения SSH сервер, по умолчанию используется 22, но в целях безопасности порт подключения ssh часто изменяют;

• имя и пароль пользователя на удаленном сервере.

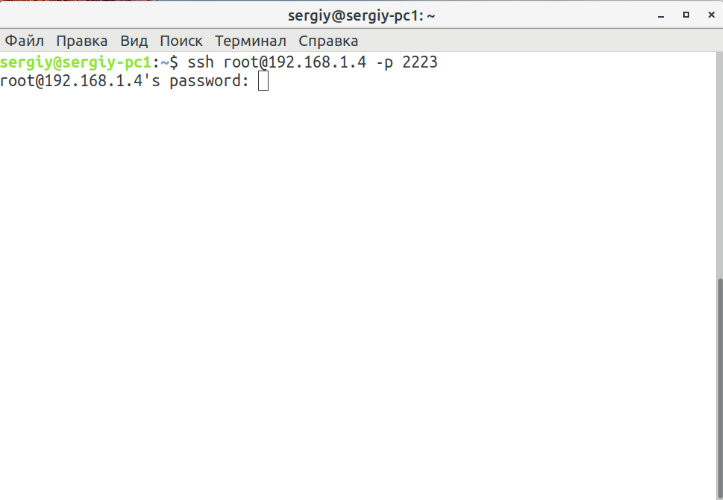
2. Для подключения к удаленному компьютеру ее синтаксис будет выглядеть следующим образом:

|  |
| --- |
| $ ssh имя\_пользователя@айпи\_адрес |

Это самый простой вариант, если вам также нужно задать порт, используйте опцию -p:

|  |
| --- |
| $ ssh имя\_пользователя@айпи\_адрес -p порт |

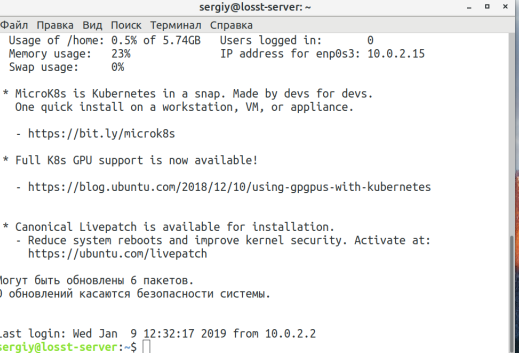
Если ip\_адрес и порт правильные, то на следующем шаге программа попросит у вас ввести пароль:



Если пытаетесь подключится через SSH к этому серверу первый раз, то утилита также попросит подтвердить добавление нового устройства в свой список известных устройств, здесь нужно набрать yes и нажать Enter:



Теперь вы подключены, и все вводимые далее команды будут выполнены на удаленном сервере:



**Windows**:

Раньше подключение по SSH из Windows выполнялось только с помощью сторонних утилит, например PuTTY. Но в Windows 10 был добавлен встроенный OpenSSH клиент и работает он точно так же, как и в Linux. По умолчанию этот компонент не активирован.

Для его установки откройте

1. Параметры -> Приложения
2. Управление дополнительными компонентами
3. Здесь нажмите добавить новый компонент и в открывшемся меню выберите OpenSSH Client и нажмите Установить:
4. Дальше вернитесь назад и дождитесь завершения установки. После того, как SSH клиент будет установлен нужно обязательно перезагрузить компьютер.

После можно использовать ssh утилиту через CMD. Синтаксис у нее такой же, как в Linux