Настройка OpenSSH доступа по Рутокен MFA

Параметры стенда

IP сервера 10.0.2.15

Имя удаленного пользователя user

Установка OpenSSH

Нам необходим OpenSSH версии 8.3 и выше, причем как на сервере так и на клиенте. Для начала попробуйте установить нужную версию OpenSSH из репозиториев. Это можно сделать с помощью команд:

```
# Debian
sudo apt-get update
sudo apt-get install openssh-client openssh-server

# Red Hat
sudo yum update
sudo yum install openssh-clients openssh-server
```

Далее узнаем, какая версия установлена с помощью команды:

```
sshd -V
```

На сервере

После того как сборка прошла успешно, в первую очередь выставим аутентификацию с использованием публичных ключей. Для этого в файле **/etc/ssh/sshd_config** раскомментируем строку

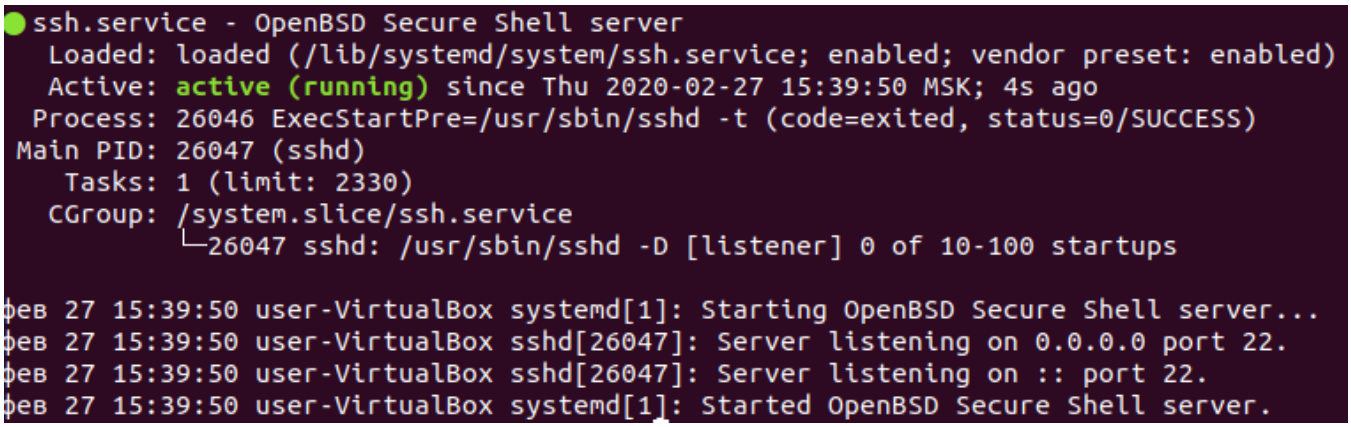
/etc/ssh/sshd_config

```
PubkeyAuthentication yes
```

Перезапускаем демона ssh и убедимся, что он запустился без ошибок

```
sudo systemctl restart sshd
sudo systemctl status sshd
```

Вывод должен быть примерно следующим:



В Red Hat возможна проблема связанная с неизвестной опцией *GSSAPIKexAlgorithms* передаваемой в качетсве аргумента sshd. Для того чтобы это исправить, нужно в файле **/etc/crypto-policies/back-ends/opensshserver.config** удалить данный аргумент и его параметры. Также в этом же файле нужно в опции PubkeyAcceptedKeyTypes нужно дописать sk-ecdsa-sha2-nistp256@openssh.com,sk-ssh-ed25519@openssh.com для прддержки аутентификации через U2F.

На клиенте

Создадим ключ на клиенте, требующий аутентификацию через U2F:

```
ssh-keygen -t ecdsa-sk
```

В процессе выполнения данной команды, токен был потребовать нажатие пользователя. Данный ключ запишется в файл внутри ФС, указанный вами, по умолчанию это $HOME/.ssh/id_rsa.pub Сгенерированный ключ копируем в файл ~/.ssh/authorized_keys лежащий на сервере

Попробуем осуществить аутентификацию (во время выполнения данной команды, должно быть взаимодействие с U2F):

```
~/.ssh$ ssh user@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ECDSA key fingerprint is SHA256:pQ4vwrTm8OwwI7uhzfbbmrvHTM5d1bvMI0j49Xr6McQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ECDSA) to the list of known hosts.
Last login: Thu Feb 27 00:08:43 2020 from 127.0.0.1
```

Как видно аутентификация прошла успешно