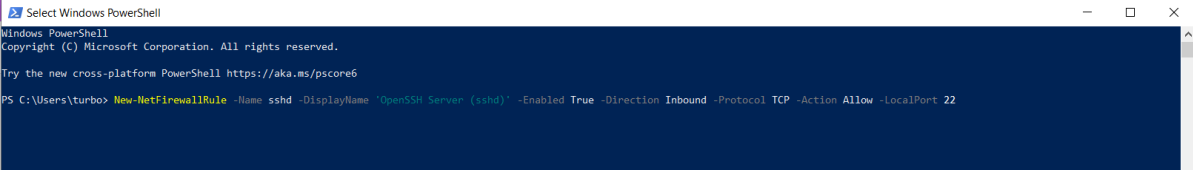# Настройка SSH

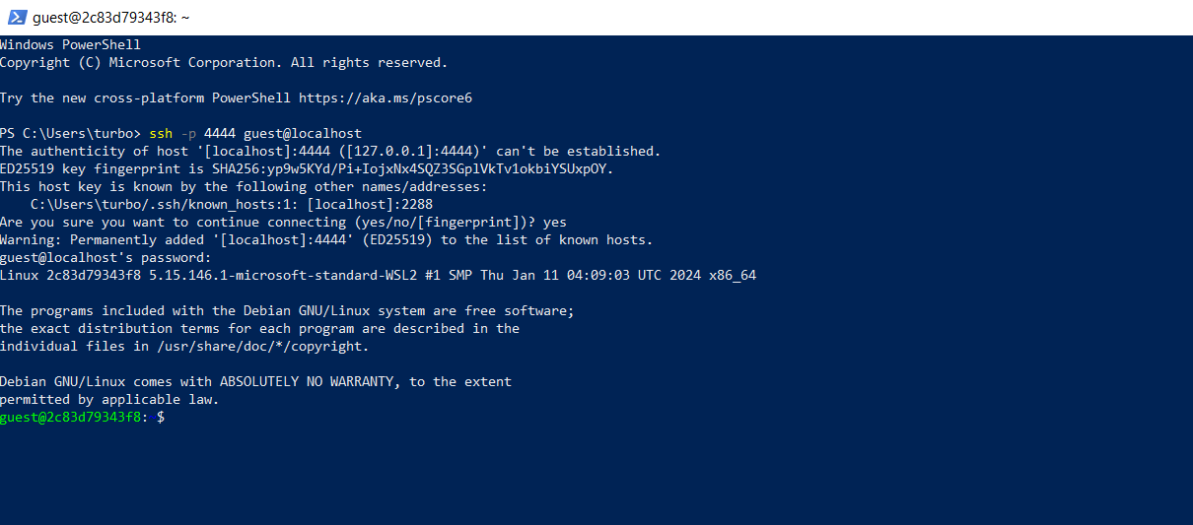## настройка файервола
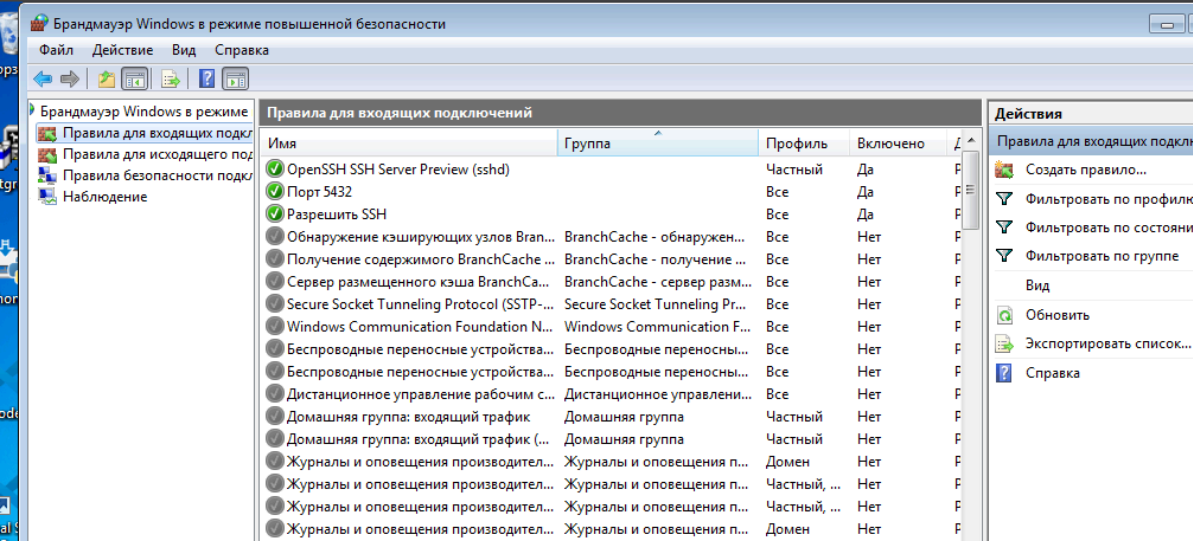

настройка соединения

```
net start sshd
```

проверка

сервер ssh

Настройка SSL

генерация ключей

> ключи можно сгенерировать следующими командами

```
# чтобы правильно отображать пути
MSYS_NO_PATHCONV=1

# генерируем основной ключ
openssl req -new -text -passout pass:12345678 -subj /C=Russia/CN=localhost -
keyout privkey.pem -out server.req

# генерируем сертификат
openssl rsa -in privkey.pem -passin pass:12345678 -out server.key
openssl req -x509 -in server.req -text -key server.key -out server.crt
```

ключи в папке

Name	Date modified	Type	Size
privkey.pem	11/24/2024 8:56 PM	PEM File	2 KB
server.crt	11/24/2024 8:56 PM	Security Certificate	5 KB
server.key	11/24/2024 8:56 PM	KEY File	2 KB
server.req	11/24/2024 8:56 PM	REQ File	4 KB

настройка внешних соединений в pg_hba

Файл   Машина   Вид   Ввод   Устройства   Справка

pg_hba.conf — Блокнот

Файл   Правка   Формат   Вид   Справка

```
# NAME=VALUE.  The available options depend on the different
# authentication methods -- refer to the "Client Authentication"
# section in the documentation for a list of which options are
# available for which authentication methods.
#
# Database and user names containing spaces, commas, quotes and other
# special characters must be quoted.  Quoting one of the keywords
# "all", "sameuser", "samerole" or "replication" makes the name lose
# its special character, and just match a database or username with
# that name.
#
# This file is read on server startup and when the server receives a
# SIGHUP signal.  If you edit the file on a running system, you have to
# SIGHUP the server for the changes to take effect, run "pg_ctl reload",
# or execute "SELECT pg_reload_conf()".
#
# Put your actual configuration here
# ----------------------------------
#
#
# If you want to allow non-local connections, you need to add more
# "host" records.  In that case you will also need to make PostgreSQL
# listen on a non-local interface via the listen_addresses
# configuration parameter, or via the -i or -h command line switches.


# TYPE   DATABASE          USER            ADDRESS                      METHOD

# IPv4 local connections:
host     all               all             127.0.0.1/32                 md5
# IPv6 local connections:
host     all               all             ::1/128                      md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
host     replication       all             127.0.0.1/32                 md5
host     replication       all             ::1/128                      md5

hostssl all all 0.0.0.0/0 md5
```

Файл   Машина   Вид   Ввод   Устройства   Справка

postgresql.conf — Блокнот

Файл   Правка   Формат   Вид   Справка

```
                                          # (change requires restart)
#unix_socket_group = ''                   # (change requires restart)
#unix_socket_permissions = 0777           # begin with 0 to use octal notation
                                          # (change requires restart)
#bonjour = off                            # advertise server via Bonjour
                                          # (change requires restart)
#bonjour_name = ''                        # defaults to the computer name
                                          # (change requires restart)

# - Security and Authentication -

#authentication_timeout = 1min            # 1s-600s
ssl = on
ssl_ciphers = 'HIGH:MEDIUM:+3DES:!aNULL' # allowed SSL ciphers
ssl_prefer_server_ciphers = on
#ssl_ecdh_curve = 'prime256v1'
#ssl_dh_params_file = ''
ssl_cert_file = 'server.crt'
ssl_key_file = 'server.key'
ssl_ca_file = 'client_ca.crt'
#ssl_crl_file = ''
#password_encryption = md5                # md5 or scram-sha-256
#db_user_namespace = off
#row_security = on
```

проверяем работу psql с сервера в защищенном режиме

```
root@163fb5a64493:/# psql -U app_user "sslmode=require dbname=wirehouse_db
> "
psql (16.2 (Debian 16.2-1.pgdg120+2))
Type "help" for help.

wirehouse_db=#
```

настройка клиента

> генерация клиентских ключей происходит подобным образом, только подписывается имя пользователя

```
# чтобы правильно отображать пути
MSYS_NO_PATHCONV=1

# генерируем основной ключ
openssl req -new -text -passout pass:12345678 -subj /C=Russia/CN=superuser -
keyout superuser.pem -out superuser.req

# генерируем сертификат
openssl rsa -in privkey.pem -passin pass:12345678 -out superuser.key
openssl req -x509 -in superuser.req -text -key superuser.key -out superuser.crt
```

проерка клиента

Name	Date modified	Type	Size
superuser.crt	11/24/2024 8:56 PM	Security Certificate	5 KB
superuser.key	11/24/2024 8:56 PM	KEY File	2 KB
superuser.pem	11/24/2024 8:56 PM	PEM File	2 KB
superuser.req	11/24/2024 8:56 PM	REQ File	4 KB

подтверждение через ssh

```
root@163fb5a64493:/# psql -U app_user "sslmode=require dbname=wirehouse_db
> "
psql (16.2 (Debian 16.2-1.pgdg120+2))
Type "help" for help.

wirehouse_db=#
```