

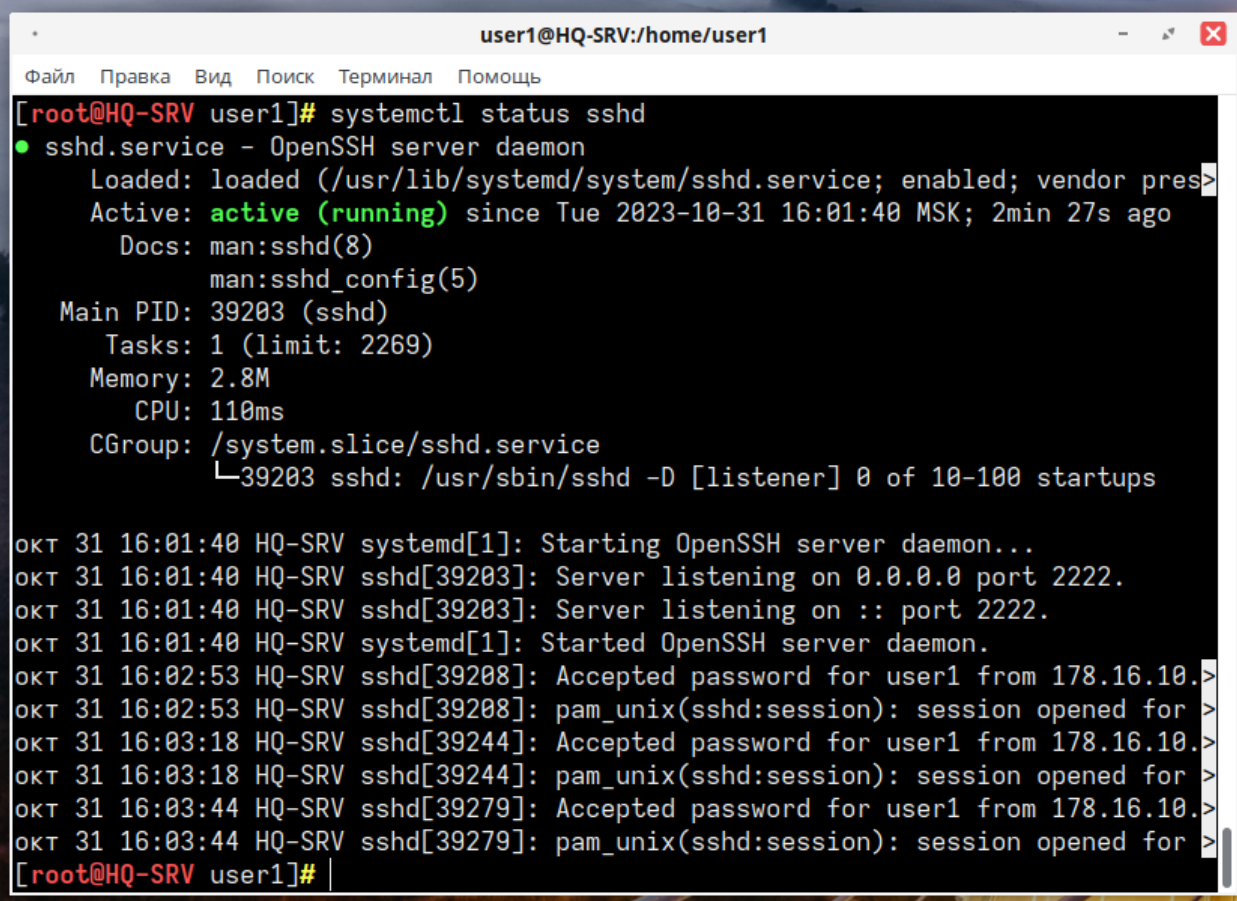
Задание.

Настройте подключение по SSH для удалённого конфигурирования устройства HQ-SRV по порту 2222. Учтите, что вам необходимо перенаправить трафик на этот порт по средствам контролирования трафика.

Настройте контроль доступа до HQ-SRV по SSH со всех устройств, кроме CLI.

Решение.

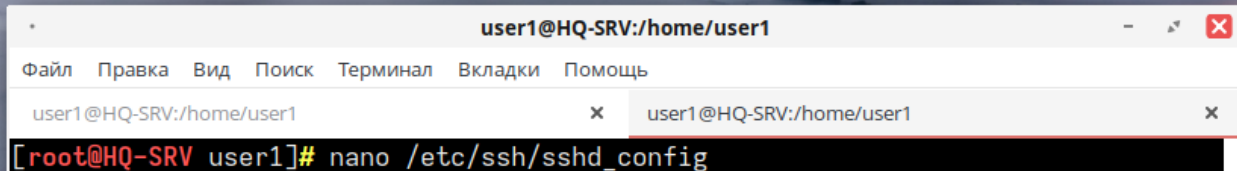
Для настройки доступа по SSH к HQ-SRV по порту 2222 необходимо проверить работу службы ssh



```
user1@HQ-SRV:/home/user1
Файл Правка Вид Поиск Терминал Помощь
[root@HQ-SRV user1]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor pres
   Active: active (running) since Tue 2023-10-31 16:01:40 MSK; 2min 27s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 39203 (sshd)
     Tasks: 1 (limit: 2269)
    Memory: 2.8M
       CPU: 110ms
   CGroup: /system.slice/sshd.service
           └─39203 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

окт 31 16:01:40 HQ-SRV systemd[1]: Starting OpenSSH server daemon...
окт 31 16:01:40 HQ-SRV sshd[39203]: Server listening on 0.0.0.0 port 2222.
окт 31 16:01:40 HQ-SRV sshd[39203]: Server listening on :: port 2222.
окт 31 16:01:40 HQ-SRV systemd[1]: Started OpenSSH server daemon.
окт 31 16:02:53 HQ-SRV sshd[39208]: Accepted password for user1 from 178.16.10.
окт 31 16:02:53 HQ-SRV sshd[39208]: pam_unix(sshd:session): session opened for
окт 31 16:03:18 HQ-SRV sshd[39244]: Accepted password for user1 from 178.16.10.
окт 31 16:03:18 HQ-SRV sshd[39244]: pam_unix(sshd:session): session opened for
окт 31 16:03:44 HQ-SRV sshd[39279]: Accepted password for user1 from 178.16.10.
окт 31 16:03:44 HQ-SRV sshd[39279]: pam_unix(sshd:session): session opened for
[root@HQ-SRV user1]#
```

Для внесения изменений настроек ssh необходимо открыть файл /etc/ssh/sshd_config



```
user1@HQ-SRV:/home/user1
Файл Правка Вид Поиск Терминал Вкладки Помощь
user1@HQ-SRV:/home/user1
user1@HQ-SRV:/home/user1
[root@HQ-SRV user1]# nano /etc/ssh/sshd_config
```

Раскомментируем строку **Port** и изменим номер порта с 22 на 2222

Добавим строку **DenyUsers** [*@3.3.3.*](#) - Данная строка запрещает доступ к серверу любому пользователю (знак * перед @ о) с любого адреса подсети 3.3.3.0 (знак * в конце адреса 3.3.3.*)

И разрешаем доступ по ssh суперпользователю root: **PermitRootLogin yes**

```
GNU nano 4.3 /etc/ssh/sshd_config Изменён
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 2222
DenyUsers *@3.3.3.*
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
# Ciphers and keying
#RekeyLimit default none
# Logging
#SyslogFacility AUTH
#LogLevel INFO
# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

^G Помощь      ^O Записать    ^W Поиск      ^K Вырезать    ^J Выровнять   ^C ТекПозиц   M-U Отмена
^X Выход      ^R ЧитФайл    ^\ Замена     ^U Paste Text  ^T Словарь    ^_ К строке   M-E Повтор
```

Сохраняем изменения в файле и выходим.

Перезагружаем службу ssh, чтобы изменения применились.

```
user1@HQ-SRV
Файл  Правка  Вид  Поиск  Терминал  Вкладки  Помощь
user1@HQ-SRV:/home/user1 x
[root@HQ-SRV user1]# systemctl restart sshd
```

Для перенаправления трафика на этот порт по средствам контролирования трафика будем использовать firewalld. Firewalld – это надстройка над встроенным файрволлом iptables.

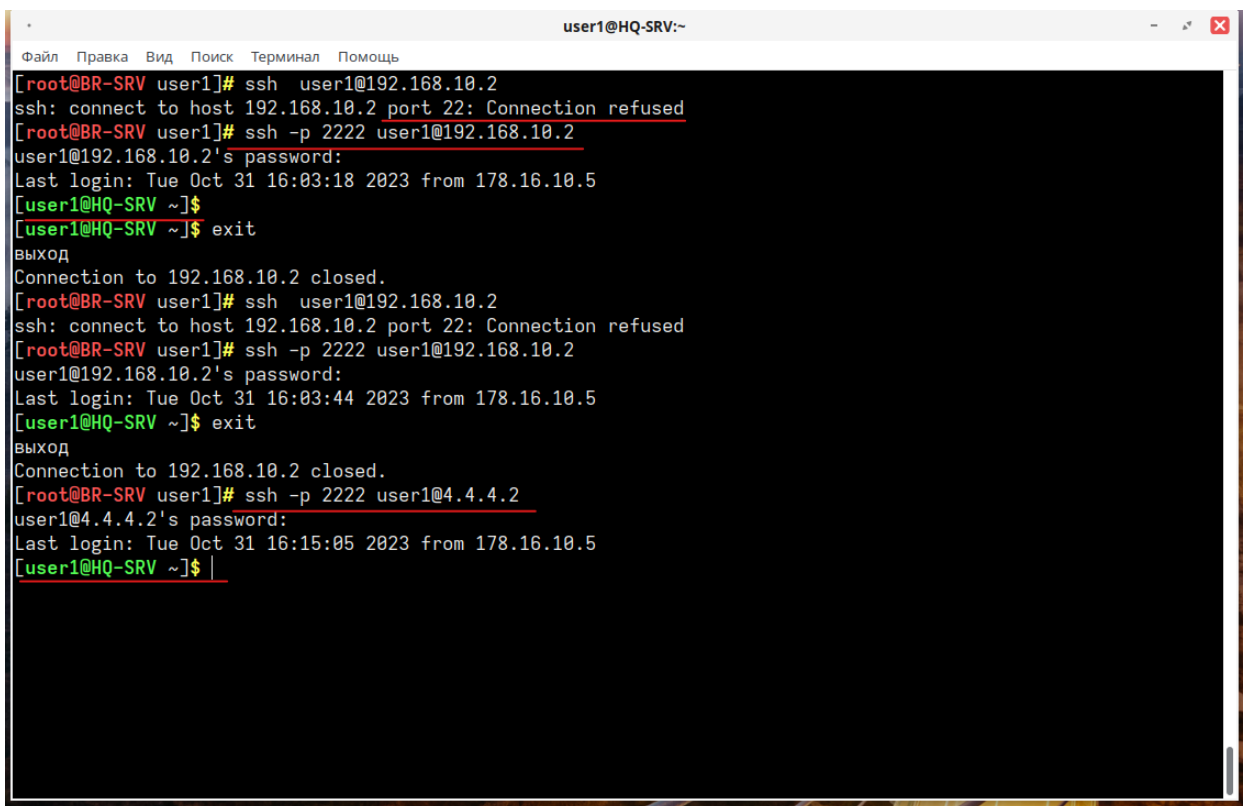
Установим firewalld (устанавливается как с DVD, так и с интернета)

```
user1@HQ-R:/home/user1
Файл  Правка  Вид  Поиск  Терминал  Помощь
[root@HQ-R user1]# yum install firewalld
```

Проверим состояние firewalld, и если надо, включаем.


```
[root@HQ-R user1]# firewall-cmd --list-all
public (active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: ens160 ens192
  sources:
  services: dhcpv6-client mdns ssh
  ports: 2222/tcp 22/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
    port=2222:proto=tcp:toport=2222:toaddr=192.168.10.2
  source-ports:
  icmp-blocks:
  rich rules:
[root@HQ-R user1]#
```

Переходим на VM BR-SRV и тестируем подключение по ssh к HQ-SRV



```
user1@HQ-SRV:~
Файл Правка Вид Поиск Терминал Помощь
[root@BR-SRV user1]# ssh user1@192.168.10.2
ssh: connect to host 192.168.10.2 port 22: Connection refused
[root@BR-SRV user1]# ssh -p 2222 user1@192.168.10.2
user1@192.168.10.2's password:
Last login: Tue Oct 31 16:03:18 2023 from 178.16.10.5
[user1@HQ-SRV ~]$
[user1@HQ-SRV ~]$ exit
выход
Connection to 192.168.10.2 closed.
[root@BR-SRV user1]# ssh user1@192.168.10.2
ssh: connect to host 192.168.10.2 port 22: Connection refused
[root@BR-SRV user1]# ssh -p 2222 user1@192.168.10.2
user1@192.168.10.2's password:
Last login: Tue Oct 31 16:03:44 2023 from 178.16.10.5
[user1@HQ-SRV ~]$ exit
выход
Connection to 192.168.10.2 closed.
[root@BR-SRV user1]# ssh -p 2222 user1@4.4.4.2
user1@4.4.4.2's password:
Last login: Tue Oct 31 16:15:05 2023 from 178.16.10.5
[user1@HQ-SRV ~]$
```

/Так же проверяем подключение по ssh с VM CLI. Видим, что доступ запрещен.

```
user1@CLI:/home/user1
Файл  Правка  Вид  Поиск  Терминал  Помощь
[root@CLI user1]# ssh -p 2222 user1@192.168.10.2
user1@192.168.10.2's password:
Permission denied, please try again.
user1@192.168.10.2's password:
Permission denied, please try again.
user1@192.168.10.2's password:

[root@CLI user1]# ssh -p 2222 user1@4.4.4.2
user1@4.4.4.2's password:
Permission denied, please try again.
user1@4.4.4.2's password:
Permission denied, please try again.
user1@4.4.4.2's password:

[root@CLI user1]#
```