Ограничение доступа SSH / IP

Способ первый. Разрешенные ip в файле **/etc/hosts.allow**. Пропишите в нём следующую строку:

```
SSHD: 127.0.0.1,192.168.0.100
```

127.0.0.1 замените на свой ip адрес.

Откройте следующий файл – **/etc/hosts.deny**:

```
SSHD: ALL
```

Теперь перезагрузите ssh командой **sudo *service ssh restart*.**

Второй способ. Ограничение доступа по ip посредством iptables.

Если у вас открытый фаервол, то нужно разрешить доступ только со своего ip и закрыть для остальных. 127.0.0.1 заменяем на свой ip.

```
iptables -A INPUT -s 127.0.0.1 -p tcp --dport 22 -j accept
iptables -A INPUT -p tcp --dport 22 -j DROP
```

Если фаервол закрыт, то нужно только разрешить доступ себе.

```
iptables -A INPUT -s 127.0.0.1 -p tcp --dport 22 -j accept
```

В обоих вариантах 127.0.0.1 нужно заменить на свой ip.