«Ядро линукс включает подсистему Netfilter (сетевой фильтр), который используется для манипулирования или решения судьбы сетевого трафика передаваемого в или через ваш сервер. Все современные решения линукс по сетевой защите используют эту систему пакетной фильтрации….Система пакетной фильтрации на уровне ядра была бы малоиспользуема администраторами без пользовательского интерфейса для ее управления. Для этого предназначен iptables…iptables — это все, что вам нужно для управления вашей сетевой защитой, если вы хорошо с ним знакомы, однако множество внешних интерфейсов доступны для упрощения этой задачи…ufw — простой Firewall.Он разработан для легкой настройки iptables и предоставляет дружественный способ создания сетевой защиты для IPv4 и IPv6….» источник

Включить/отключить ufw:

```
sudo ufw enable/disable
```

Открыть/закрыть порт 22 всем:

```
sudo ufw allow/deny 22
```

Удалить правило:

```
sudo ufw delete deny 22
```

Разрешить доступ к 22 порту с определенного хоста:

```
sudo ufw allow proto tcp from 10.0.0.1 to any port 22
```

Разрешить доступ к 22 порту с определенной подсети:

```
sudo ufw allow proto tcp from 10.0.1.0/24 to any port 22
```

Посмотреть статус защиты:

```
sudo ufw status
```

Полное отображение информации:

```
sudo ufw status verbose
```

Включить/отключить журналирование:

```
sudo ufw logging on/off
```