Разрешу только нужные порты:

```
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
sudo ufw allow 22/tcp
sudo ufw allow 8080/tcp
sudo ufw enable
```

Последним шагом установлю Fail2Ban для защиты от брутфорс-атак, особенно на SSH.

```
sudo apt update
sudo apt install fail2ban
```

Шаг 2: Запуск и автозапуск.

```
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
```

Проверка статуса.

```
sudo systemctl status fail2ban
```

Шаг 3: Базовая настройка (SSH)

Создай локальную конфигурацию на основе стандартного:

```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Откройте файл для редактирования:

```
sudo nano /etc/fail2ban/jail.local
```

Настрою секцию sshd.

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 2
bantime = 3600
findtime = 600
```

maxretry: сколько раз можно ввести неправильный пароль до блокировки

bantime: на сколько секунд заблокировать IP (3600 сек = 1 час)

findtime: за какой период считать неудачные попытки

Шаг 4: Перезапуск Fail2Ban

```
sudo systemctl restart fail2ban
```

Шаг 5: Проверка работы. Показать список активных «тюрем»:

```
sudo fail2ban-client status
```

Посмотреть состояние конкретной «тюрьмы» (например, SSH):

```
sudo fail2ban-client status sshd
```