

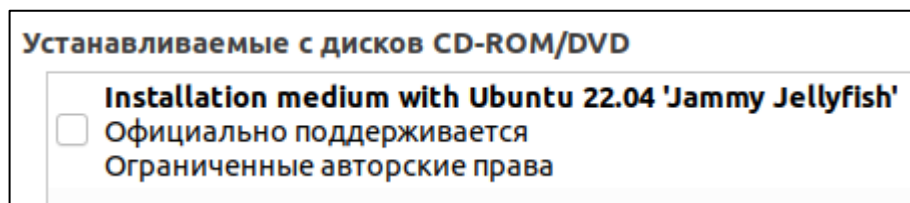
## Настройка политики безопасности Linux

Настройка политики безопасности в Linux Ubuntu будет состоять из 3 основных пунктов:

1. Настройка общей памяти
2. Настройка доступа к общему каталогу
3. Настройка Брандмауэра

Они позволят защитить системные бреши системы от вредоносных программ и пользователей.

Версия Linux Ubuntu: 22.04 “Jammy Jellyfish”.



### 1. Настройка общей памяти

По умолчанию весь объем общей памяти `/run/shm` доступен для чтения и записи с возможностью выполнения программ. Это считается брешью в безопасности для атак на запущенные сервисы. Для большинства настольных, а особенно серверных устройств рекомендуется монтировать этот файл в режиме только для чтения.

#### 1.1. Открыть файловый менеджер

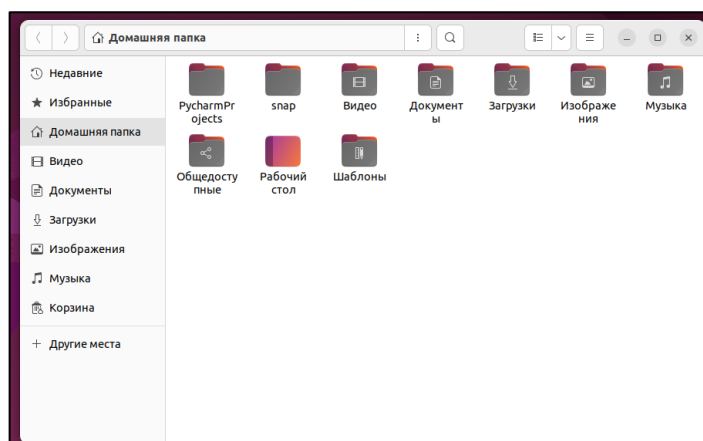


Рисунок 1.1.1 – ярлык терминала

1.2. Нажимаем комбинацию клавиш Ctrl + L и вводим /etc/fstab, чтобы открыть папку с конфигурационными файлами

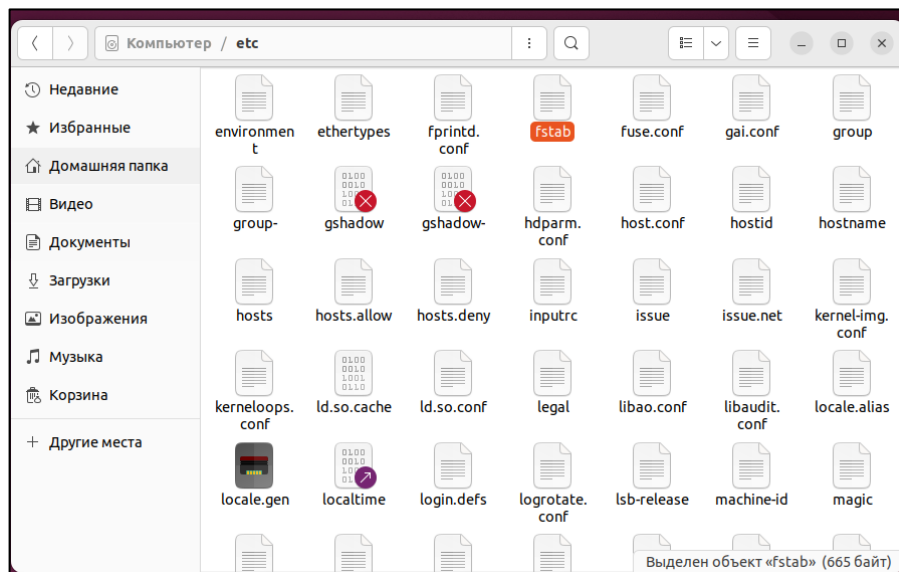


Рисунок 1.2 – содержимое папки fstab

1.3. Теперь откроем через терминал папку. Для этого введем команду \$ sudo nano /etc/fstab.

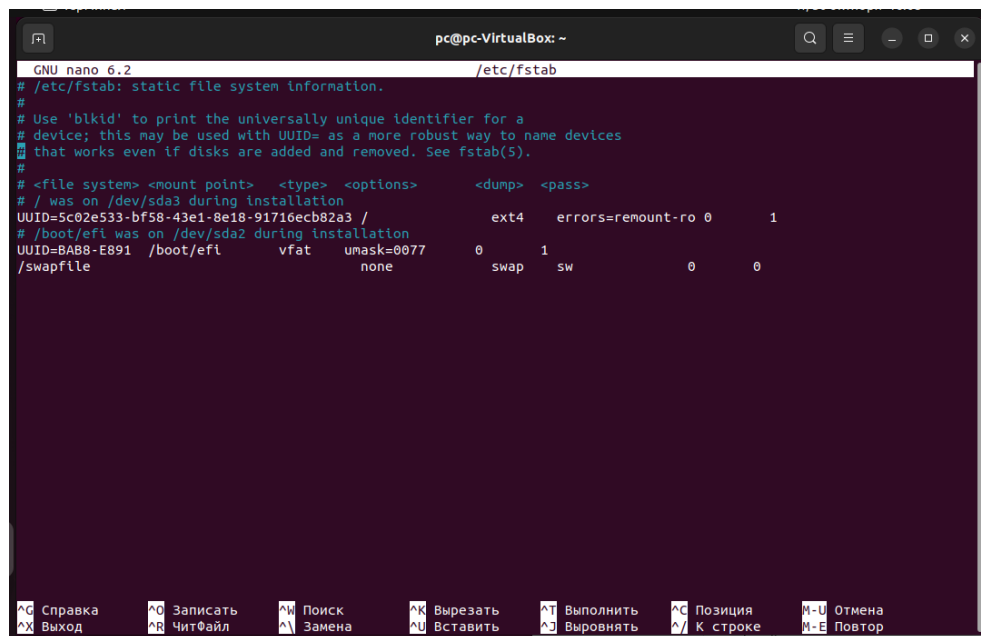


Рисунок 1.3 – папка fstab через терминал

1.4. Введем в конец файла команду. После чего сохраним файл.

```
none /run/shm tmpfs defaults,ro 0 0
```

Рисунок 1.4 – ввод команды в терминал

## 2. Настройка доступа к общему каталогу

В стандартной версии ОС, домашний каталог доступен любому пользователю, т.е. любой пользователь сможет получить доступ к личным данным.

### 2.1 Открыть терминал

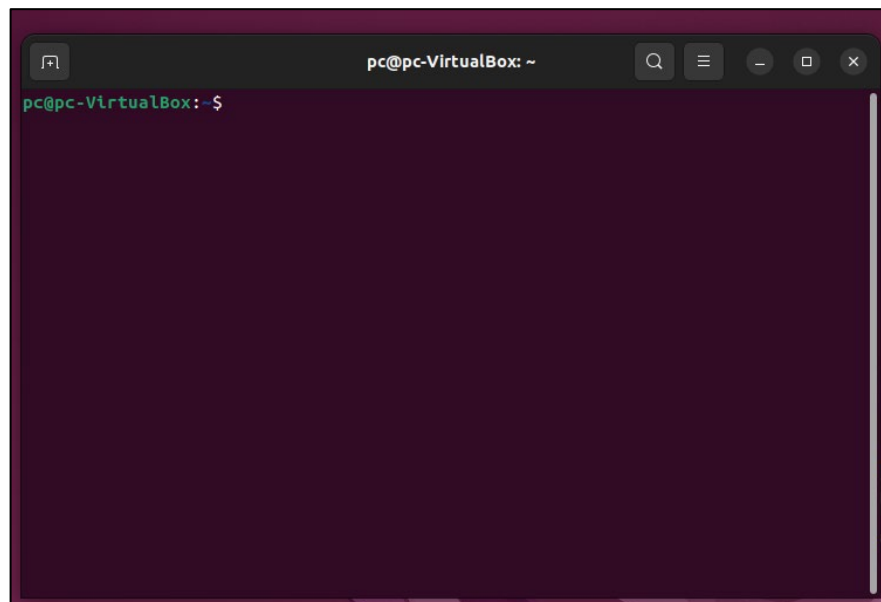


Рисунок 2.1 – окно терминала

2.1.1 Ввести команду \$ `chmod 0700 /home/имя_пользователя`, если нам необходимо, чтобы доступ к папке был только у нашего пользователя.

```
pc@pc-VirtualBox:~$ chmod 0700 /home/pc
```

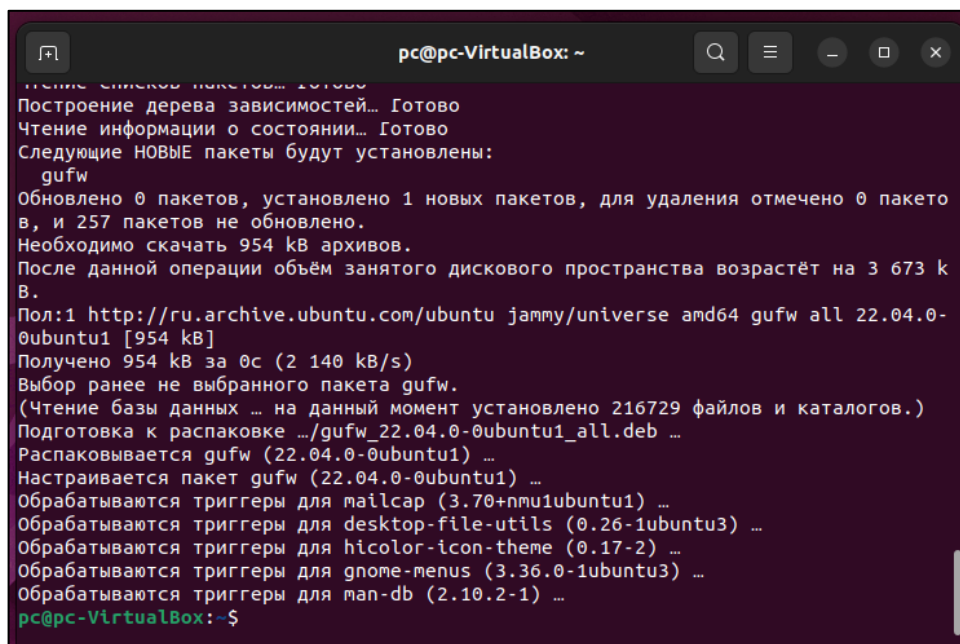
Рисунок 2.1.1 – ввод команды в терминал

2.1.2 Ввести команду \$ `chmod 0750 /home/имя_пользователя`, если нам необходимо, чтобы доступ к папке был только у администраторов.

### 3. Настройка Брандмауэра

Чтобы предотвратить несанкционированный доступ к системе нужно установить брандмауэр. В Ubuntu рекомендуется использовать gufw, так как он разработан специально для этой системы. Gufw – мощный файрвол, как брандмауэр в Windows.

#### 3.1 Открываем терминал и вводим команду `sudo apt install gufw`.



```
pc@pc-VirtualBox: ~  
Построение дерева зависимостей... Готово  
Чтение информации о состоянии... Готово  
Следующие НОВЫЕ пакеты будут установлены:  
  gufw  
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов,  
и 257 пакетов не обновлено.  
Необходимо скачать 954 kB архивов.  
После данной операции объем занятого дискового пространства возрастёт на 3 673 kB.  
Пол:1 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 gufw all 22.04.0-0ubuntu1 [954 kB]  
Получено 954 kB за 0с (2 140 kB/s)  
Выбор ранее не выбранного пакета gufw.  
(Чтение базы данных ... на данный момент установлено 216729 файлов и каталогов.)  
Подготовка к распаковке .../gufw_22.04.0-0ubuntu1_all.deb ...  
Распаковывается gufw (22.04.0-0ubuntu1) ...  
Настраивается пакет gufw (22.04.0-0ubuntu1) ...  
Обрабатываются триггеры для mailcap (3.70+nmu1ubuntu1) ...  
Обрабатываются триггеры для desktop-file-utils (0.26-1ubuntu3) ...  
Обрабатываются триггеры для hicolor-icon-theme (0.17-2) ...  
Обрабатываются триггеры для gnome-menus (3.36.0-1ubuntu3) ...  
Обрабатываются триггеры для man-db (2.10.2-1) ...  
pc@pc-VirtualBox:~$
```

Рисунок 3.1.1 – успешная установка gufw

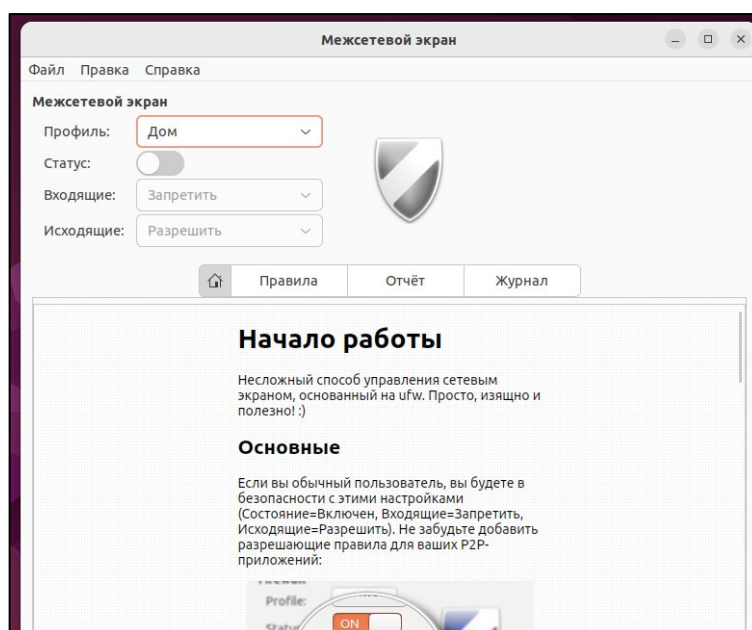


Рисунок 3.1.2 – главное окно gufw

### 3.2 Включить ограничение входящего и исходящего трафика.

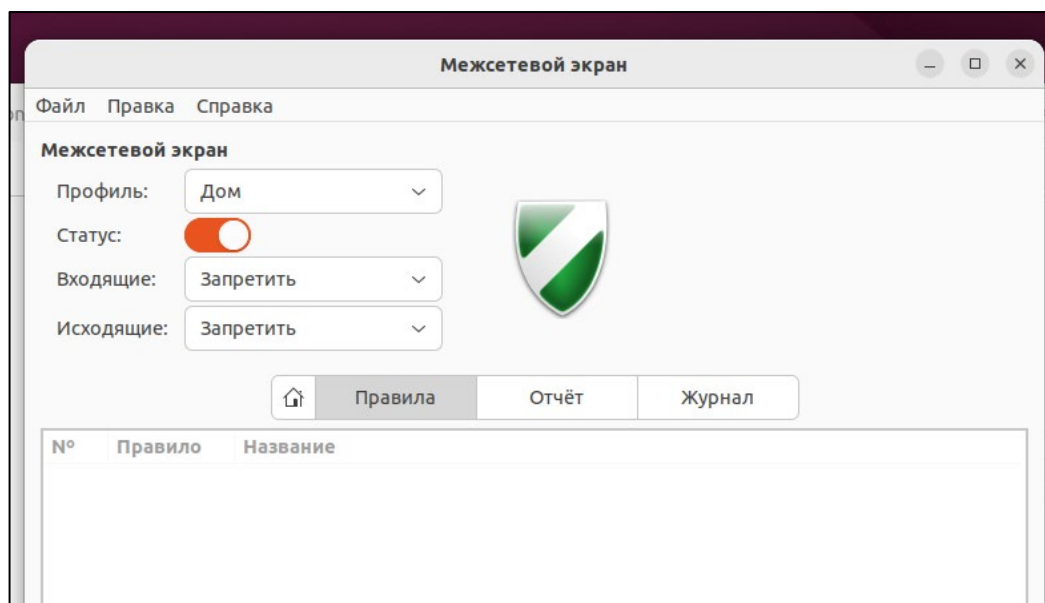


Рисунок 3.2 – включенный режим защиты

### 3.3 Проверим доступ через команду ping.

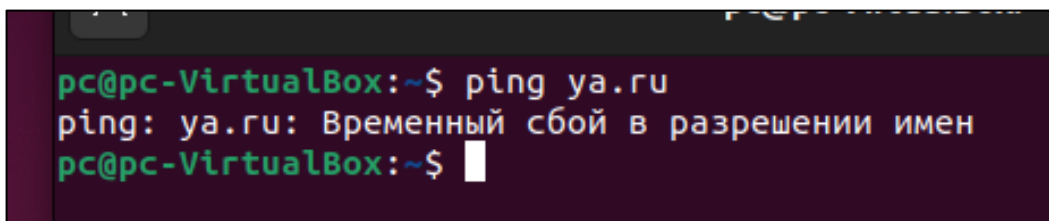


Рисунок 3.3.1 – команда ping

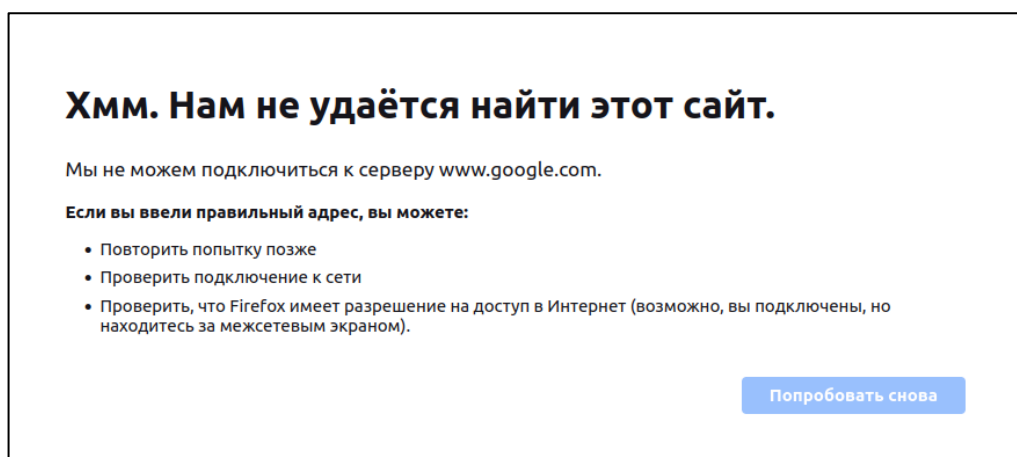


Рисунок 3.3.2 – нет доступа к сети

### 3.4 Добавим правило для доступа к DNS.

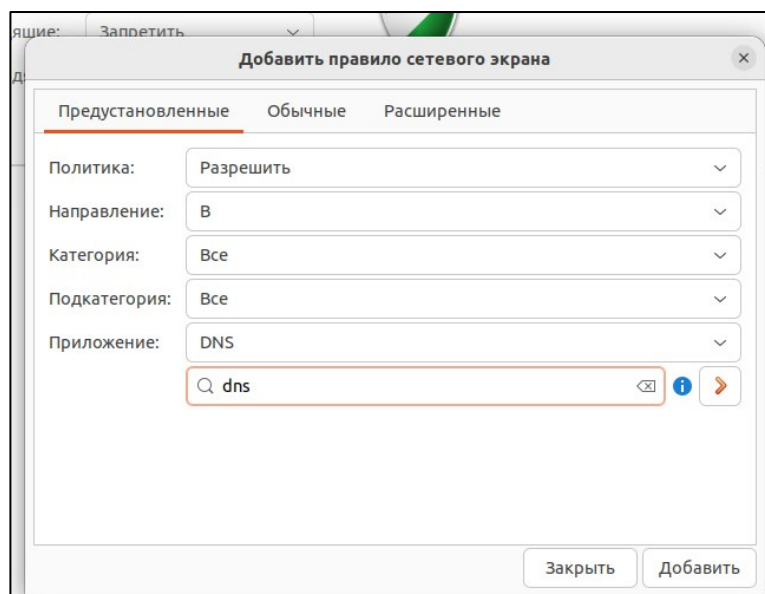


Рисунок 3.4 – добавление правила доступа к DNS

### 3.5 Добавим правило для доступа к интернету по http и https протоколам.

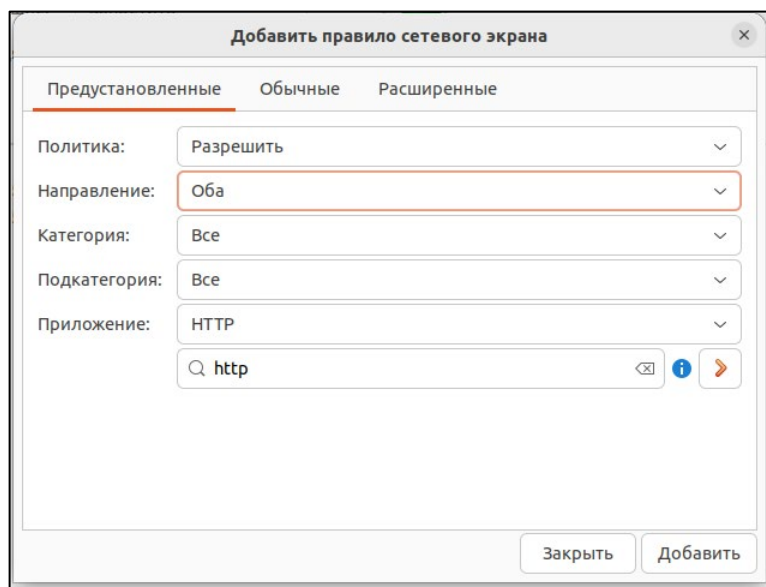


Рисунок 3.5.1 – добавление правила доступа по http

№	Правило	Название
1	53 РАЗРЕШИТЬ В Откуда угодно	DNS
2	80/tcp РАЗРЕШИТЬ В Откуда угодно	HTTP
3	80/tcp РАЗРЕШИТЬ ИЗ Откуда угодно (из)	HTTP
4	443/tcp РАЗРЕШИТЬ В Откуда угодно	HTTPS
5	443/tcp РАЗРЕШИТЬ ИЗ Откуда угодно (из)	HTTPS
6	53 (v6) РАЗРЕШИТЬ В Откуда угодно (v6)	DNS
7	80/tcp (v6) РАЗРЕШИТЬ В Откуда угодно (v6)	HTTP
8	80/tcp (v6) РАЗРЕШИТЬ ИЗ Откуда угодно (v6) (из)	HTTP
9	443/tcp (v6) РАЗРЕШИТЬ В Откуда угодно (v6)	HTTPS
10	443/tcp (v6) РАЗРЕШИТЬ ИЗ Откуда угодно (v6) (из)	HTTPS

Рисунок 3.5.2 – созданный набор правил

## Вывод

У нас получилось ограничить доступ к домашней папке, общей памяти и сделать контролируемый доступ к сети через gufw файрволл. Мы смогли сделать контролируемый доступ к Linux Ubuntu.