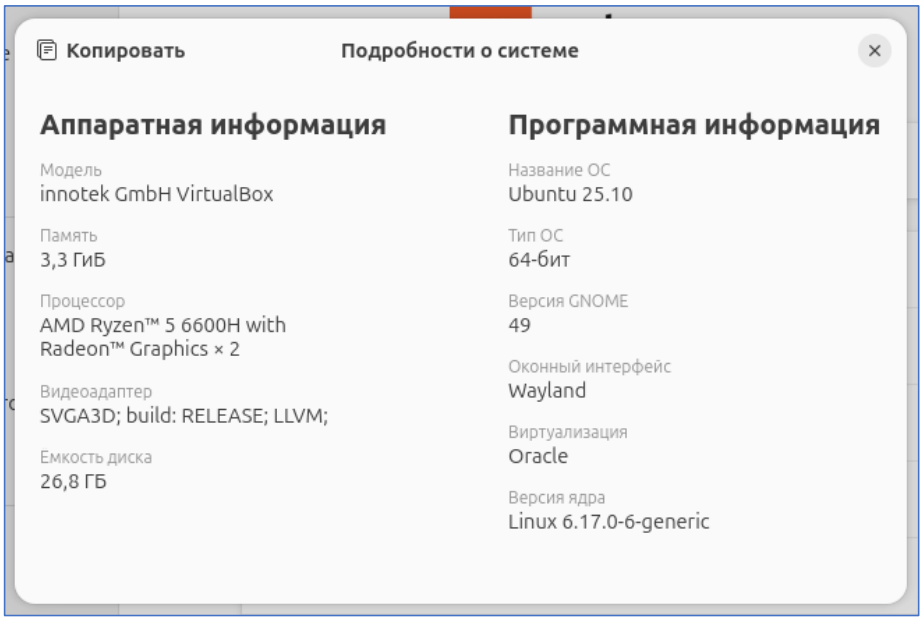
Настройка политики безопасности Linux

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: 25.10.



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

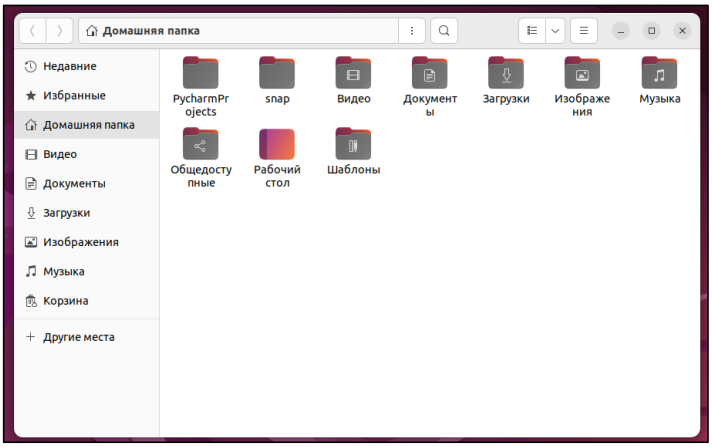


Рисунок 1.1.1 – Ярлык терминала

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

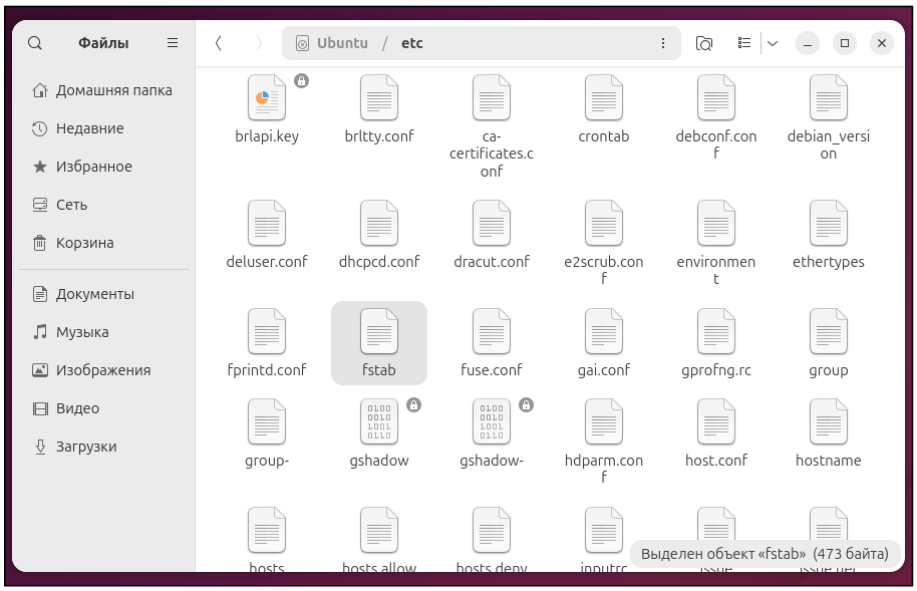


Рисунок 1.2 – Содержимое папки fstab

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

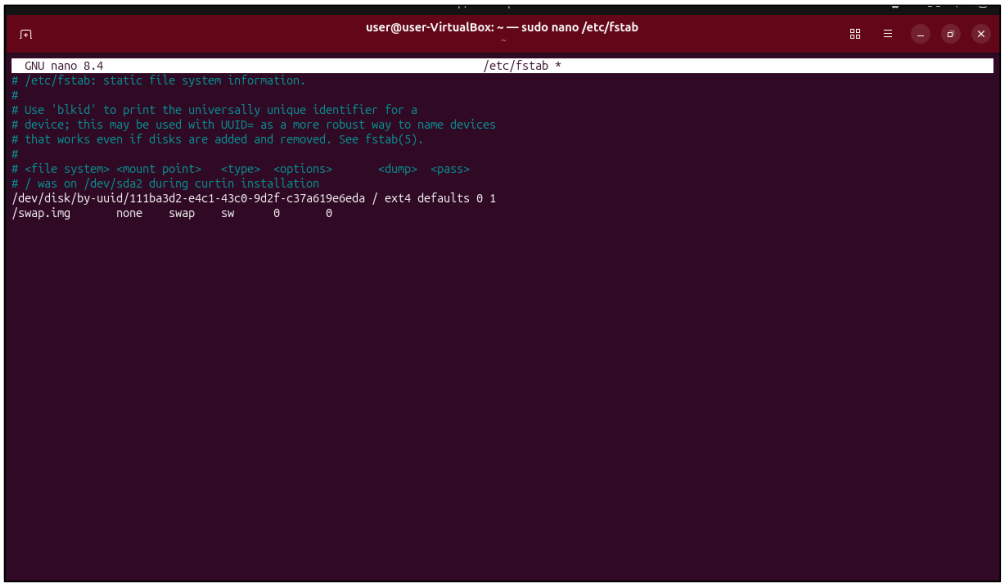


Рисунок 1.3 – Папка fstab через терминал

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 сможем 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.

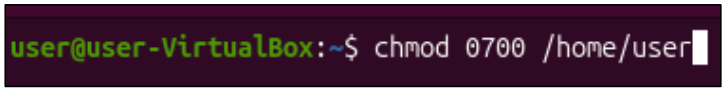


Рисунок 2.1.1 – Ввод команды в терминал

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.

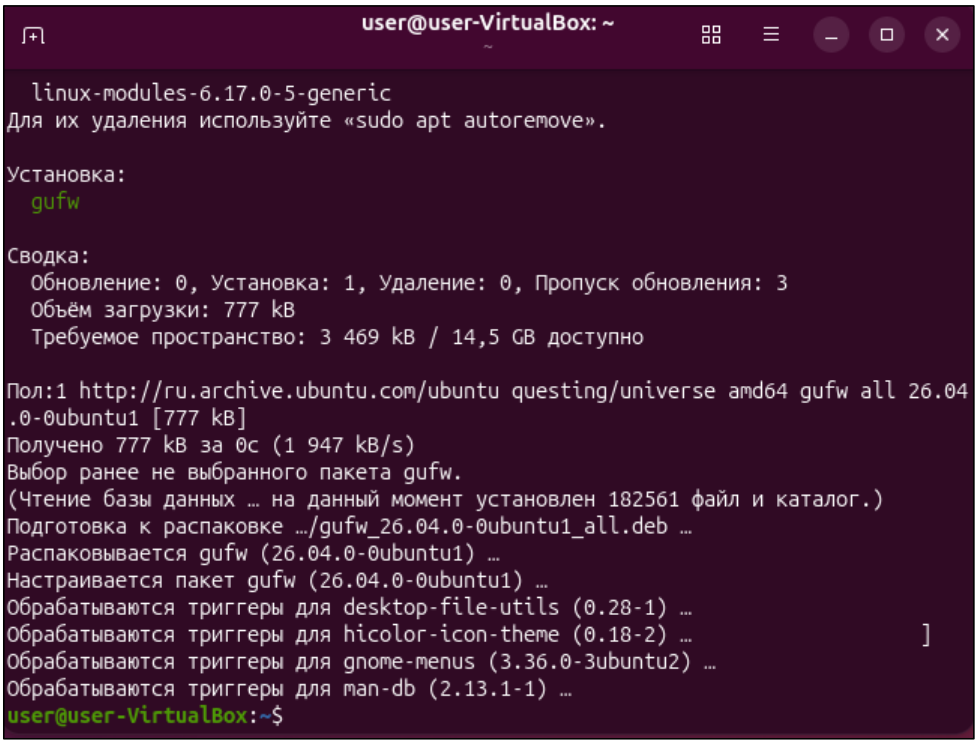


Рисунок 3.1.1 – Успешная установка gufw

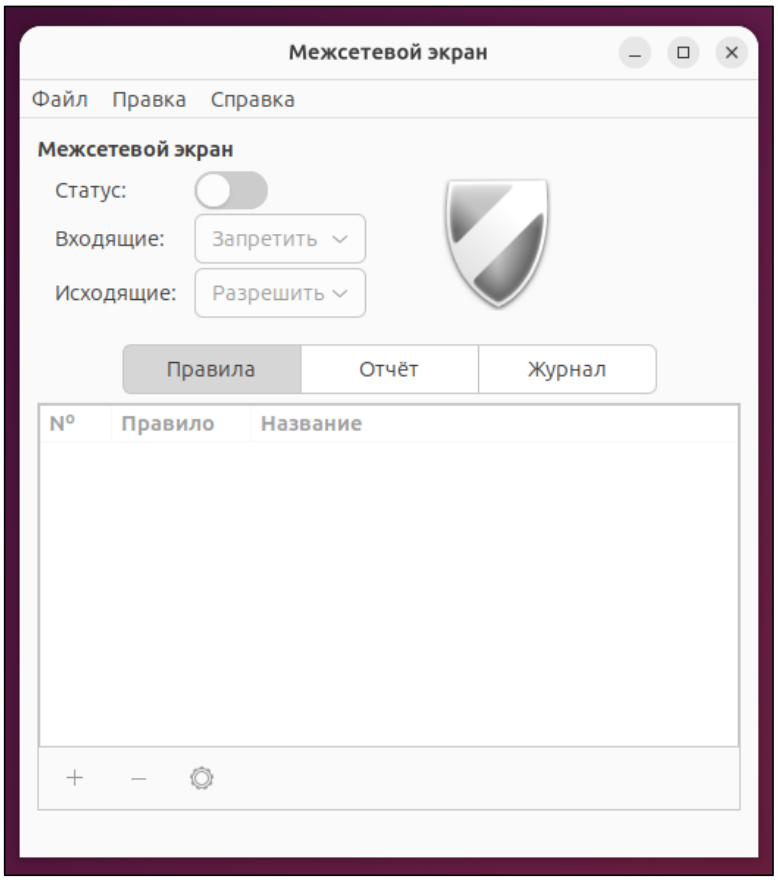


Рисунок 3.1.2 – Главное окно gufw

3.2 Включить ограничение входящего и исходящего трафика.

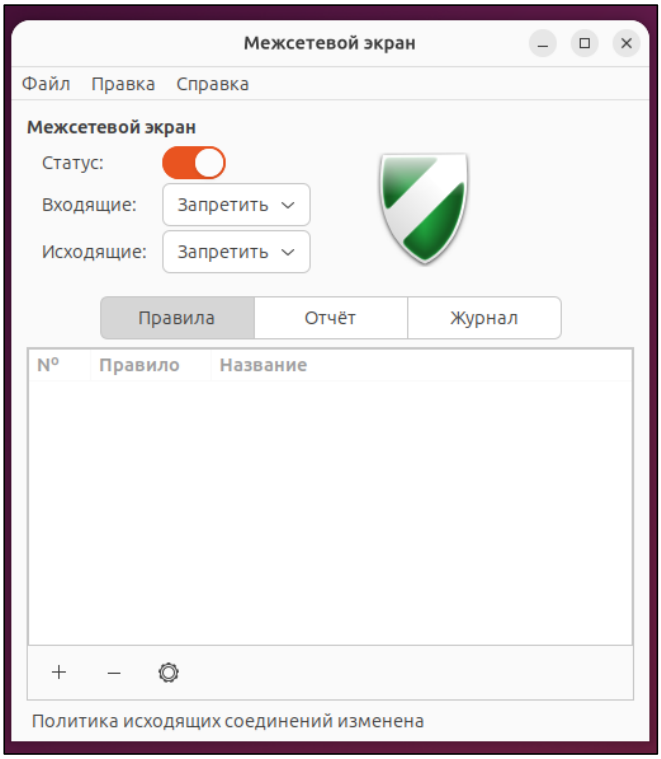


Рисунок 3.2 – Включенный режим защиты

3.3 Проверим доступ через команду ping.

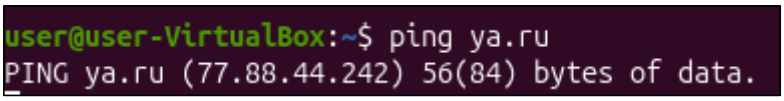


Рисунок 3.3.1 – Команда ping

Рисунок 3.3.2 – Нет доступа к сети

3.4 Добавим правило для доступа к DNS.

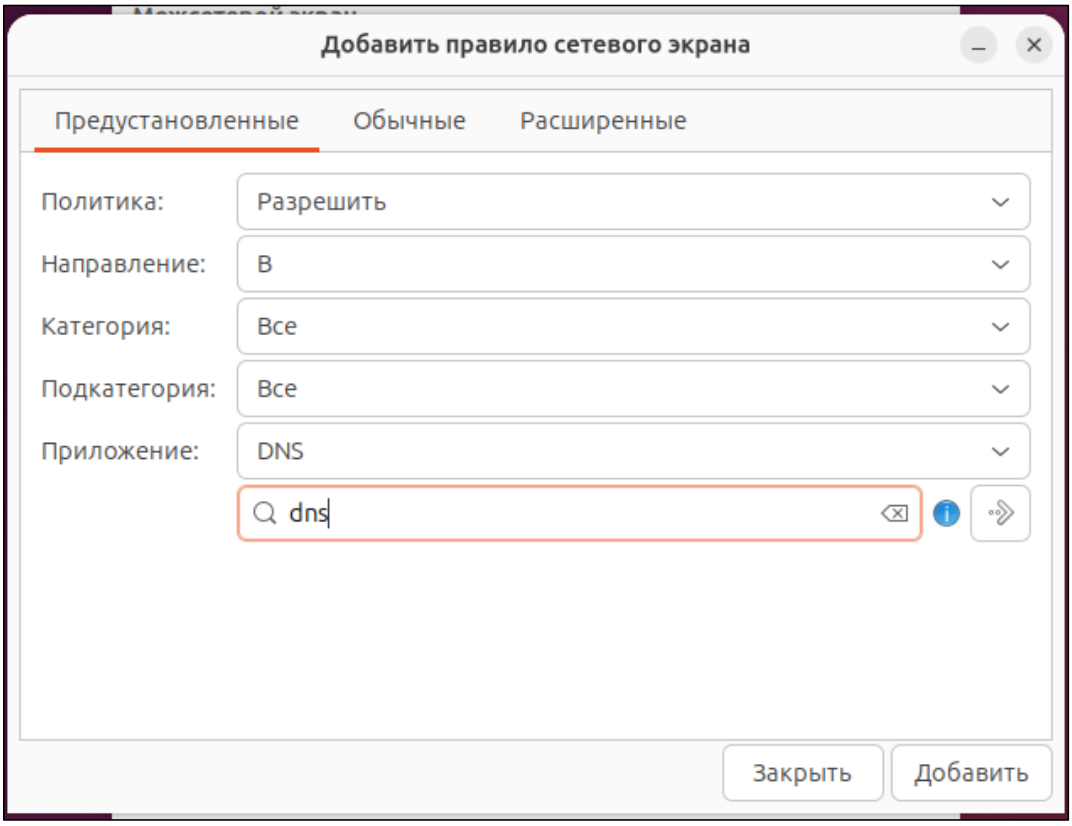


Рисунок 3.4 – Добавление правила доступа к DNS

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

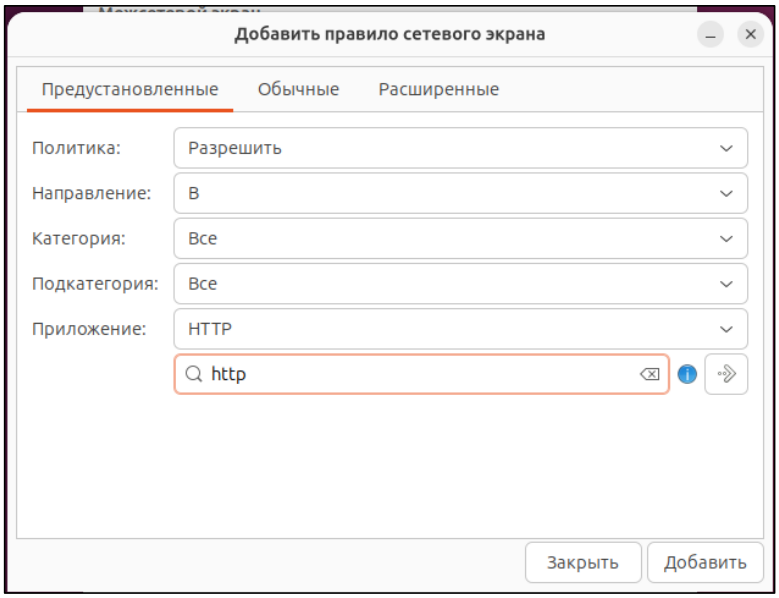


Рисунок 3.5.1 – Добавление правила доступа по http

№	Правило	Название
1	53 РАЗРЕШИТЬ В Откуда угодно	DNS
2	80/tcp РАЗРЕШИТЬ В Откуда угодно	HTTP
3	443/tcp РАЗРЕШИТЬ В Откуда угодно	HTTPS
4	53 (v6) РАЗРЕШИТЬ В Откуда угодно (v6)	DNS
5	80/tcp (v6) РАЗРЕШИТЬ В Откуда угодно (v6)	HTTP
6	443/tcp (v6) РАЗРЕШИТЬ В Откуда угодно (v6)	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.