Настройка безопасности политики Linux

Настройка будет проводиться в Ubuntu будет состоять из 2 пунктов:

1. Защита домашнего каталога и запрет входа по SSH
2. Настройка Брандмауэра

С их помощью сможем обезопасить систему от неутвержденных действий пользователей или ПО.

1. Защита домашнего каталога

По умолчанию домашний каталог доступен другим пользователям системы. Это означает, кто-то с гостевой учётной записью, может получить доступ к вашим личным файлам. Чтобы сделать каталог доступным только основному пользователю, необходимо выполнить в терминале команду, которая устанавливает права доступа, разрешающие полный доступ только владельцу, блокируя просмотр содержимого для всех остальных.

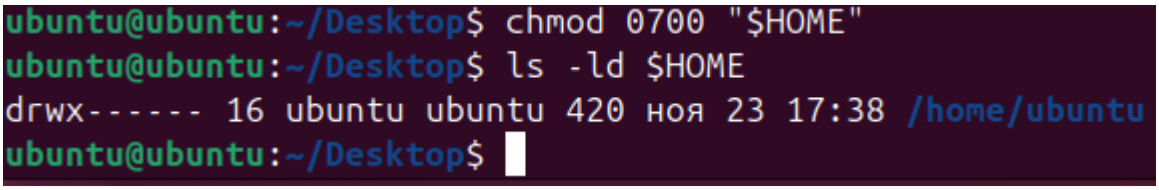

Рисунок 1.1 – Ввод команды для защиты каталога.

Запрет входа по SSH

Разрешение на вход по SSH под учётной записью root представляет угрозу безопасности. Любой сторонний пользователь может подобрать простой пароль и получить нежелательный полный контроль над системой.

Необходимо отключить эту возможность. Перед выполнением убедитесь, что на вашем компьютере установлен и запущен SSH-сервер. Если при попытке подключения вы получаете ошибку connection refused, значит, сервер не установлен, и этот шаг можно пропустить.

```
ubuntu@ubuntu:~/Desktop$ ssh localhost
ssh: connect to host localhost port 22: Connection refused
ubuntu@ubuntu:~/Desktop$
```

Рисунок 1.2 – Проверка SSH сервера.

2. Настройка Брандмауэра

2.1 Установка и запуск брандмауэр

Брандмауэр — это система, которая выступает в роли барьера между двумя сетями для защиты от угроз. Для Ubuntu используем команду gufw, так как он разработан специально для этой системы.

```
ubuntu@ubuntu:~/Desktop$ sudo apt install gufw
Чтение списков пакетов… Готово
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 пакето
в, и 194 пакетов не обновлено.
Необходимо скачать 944 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 3 748 k
B.
Пол:1 http://archive.ubuntu.com/ubuntu noble/universe amd64 gufw all 24.04.0-2 [
944 kB]
Получено 944 kB за 1с (654 kB/s)
Выбор ранее не выбранного пакета gufw.
(Чтение базы данных … на данный момент установлено 212979 файлов и каталогов.)
Подготовка к распаковке …/gufw_24.04.0-2_all.deb …
Распаковывается gufw (24.04.0-2) …
Настраивается пакет gufw (24.04.0-2) …
Обрабатываются триггеры для desktop-file-utils (0.27-2build1) …
Обрабатываются триггеры для hicolor-icon-theme (0.17-2) …
Обрабатываются триггеры для gnome-menus (3.36.0-1.1ubuntu3) …
Обрабатываются триггеры для man-db (2.12.0-4build2) …
ubuntu@ubuntu:~/Desktop$
```

Рисунок 2.1 – Ввод команды “sudo apt install gufw” для установки.

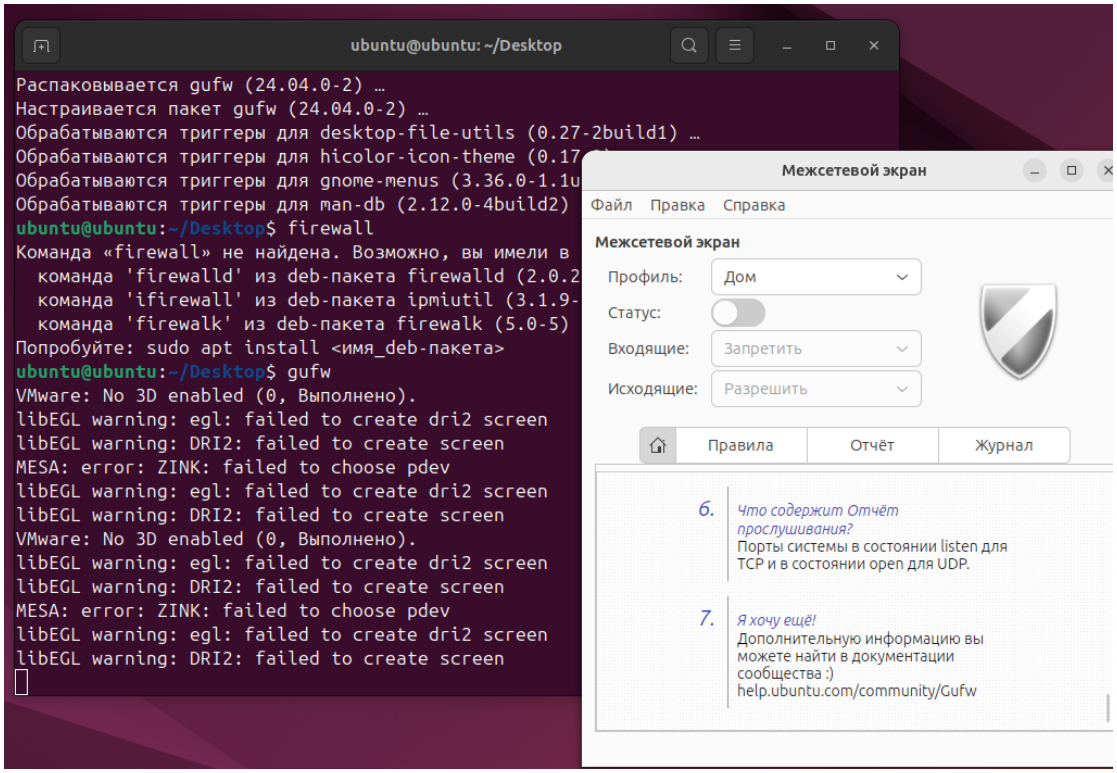

Рисунок 2.2 – Ввод команды “gufw” для запуска.

2.2 Активируем защиту

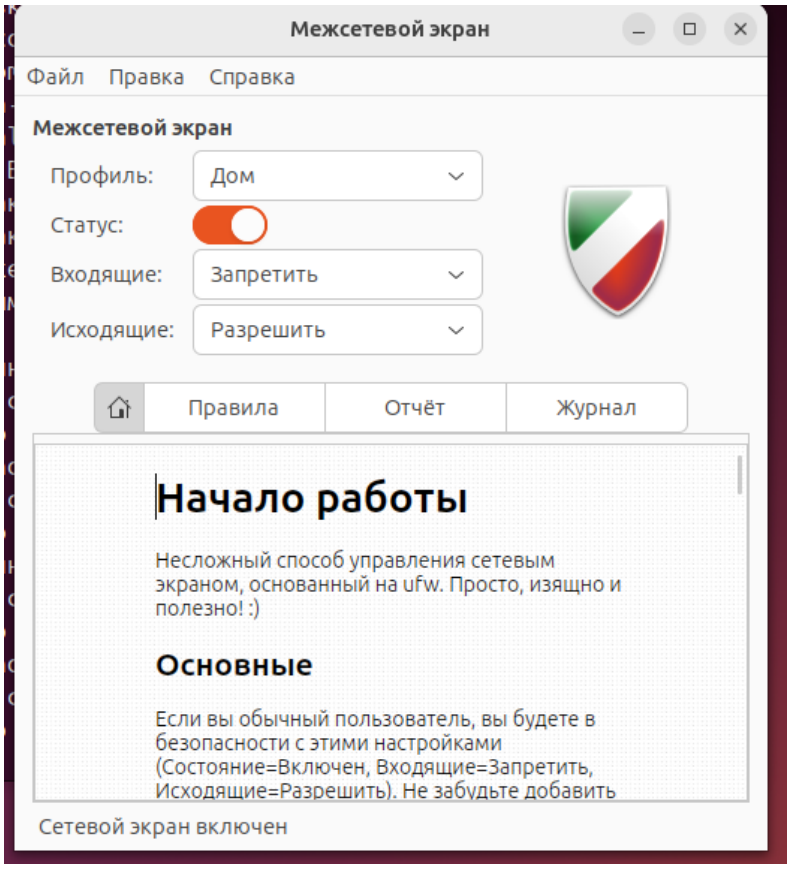

Рисунок 2.3 – Ввод команды “gufw” для запуска.

2.3 Вручную разрешаем только те порты, которые необходимы для работы доверенных программ. После включения строгой блокировки весь интернет-трафик, включая DNS-запросы, будет заблокирован.

```
ubuntu@ubuntu:~$ ping ya.ru
PING ya.ru (5.255.255.242) 56(84) bytes of data.
```

Рисунок 2.4 – Проверка блокировки интернет трафика.

Чтобы это исправить, добавьте новое правило, выберите политику «Разрешить» для DNS-трафика.

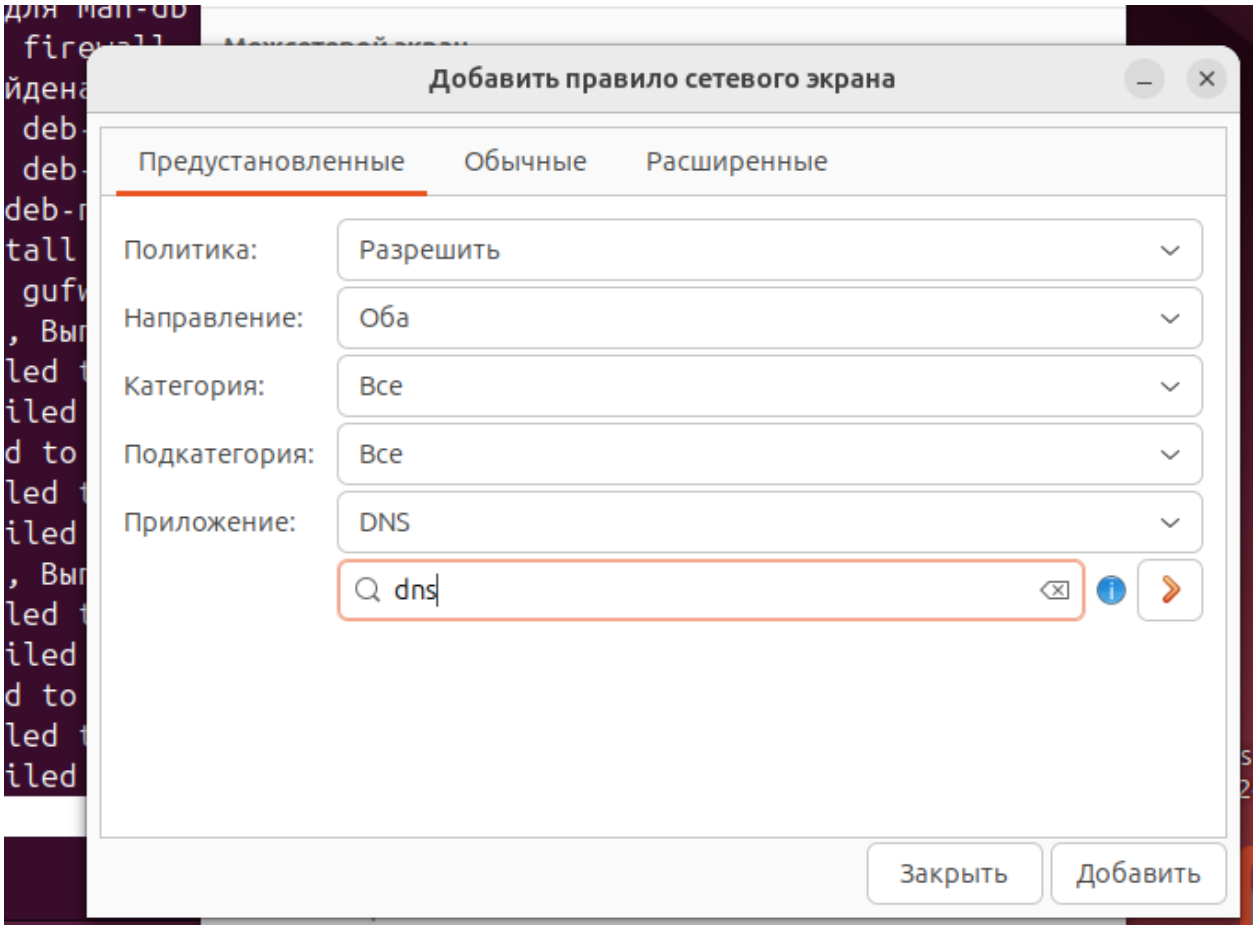

Рисунок 2.5 – Создание правило для DNS-трафика.

после добавления правила проверяем, восстановился ли доступ к интернету.

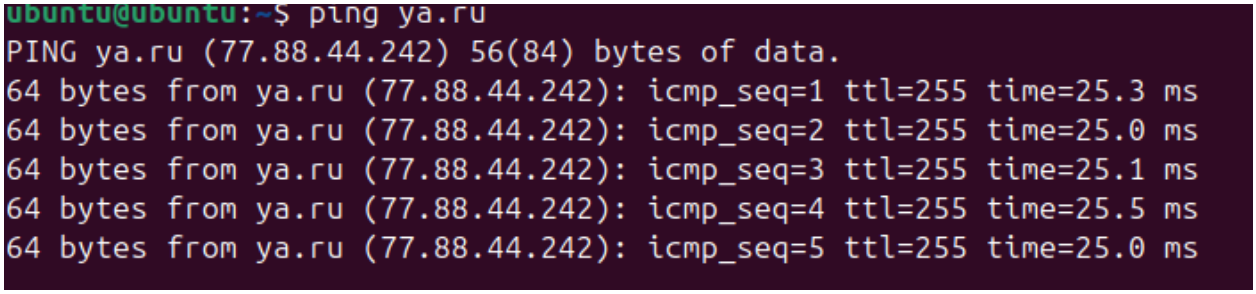

Рисунок 2.6 – Результат создания правила.