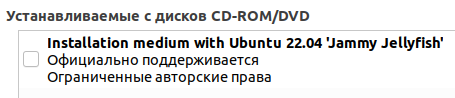
Настройка политики безопасности Linux

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. Открыть файловый менеджер

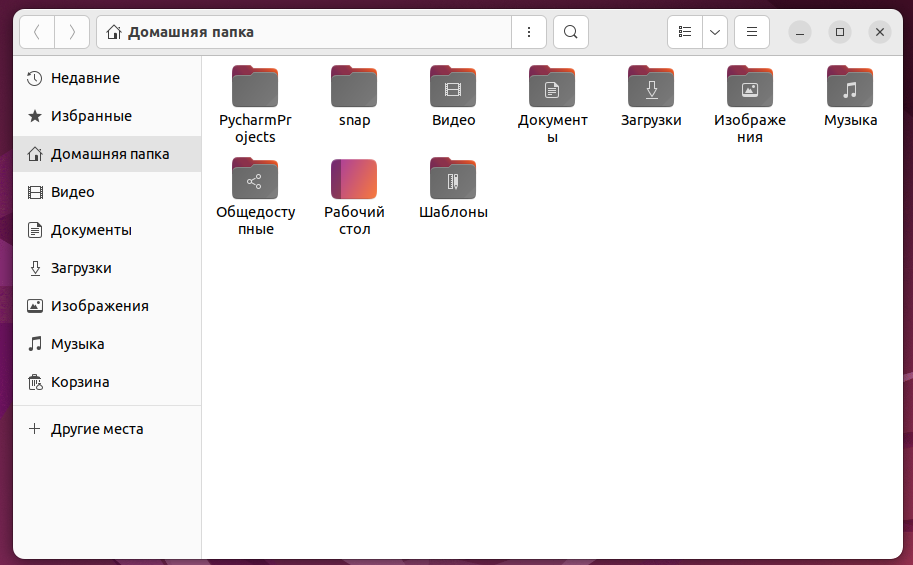


Рисунок 1.1.1 – ярлык терминала

* 1. Нажимаем комбинацию клавиш Ctrl + L и вводим /etc/fsnab, чтобы открыть папку с конфигурационными файлами

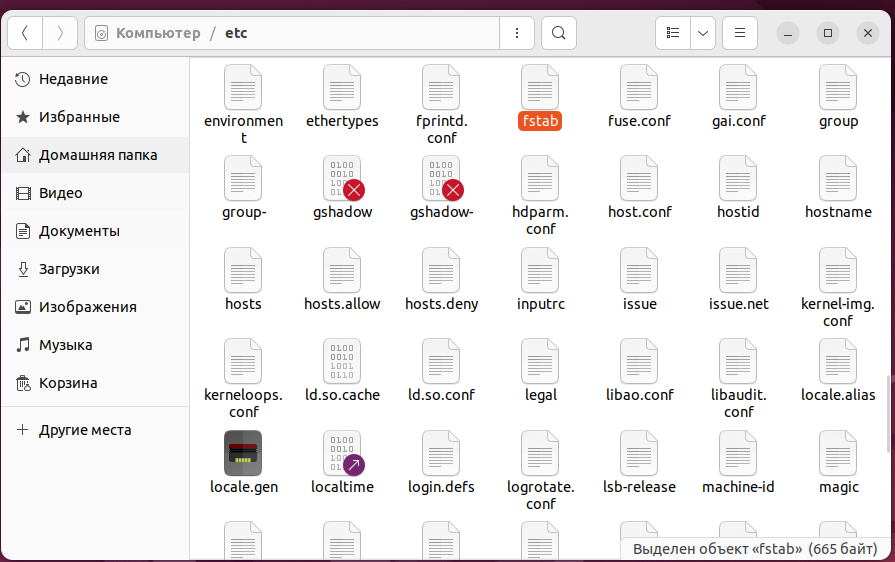


Рисунок 1.2 – содержимое папки fsnab

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

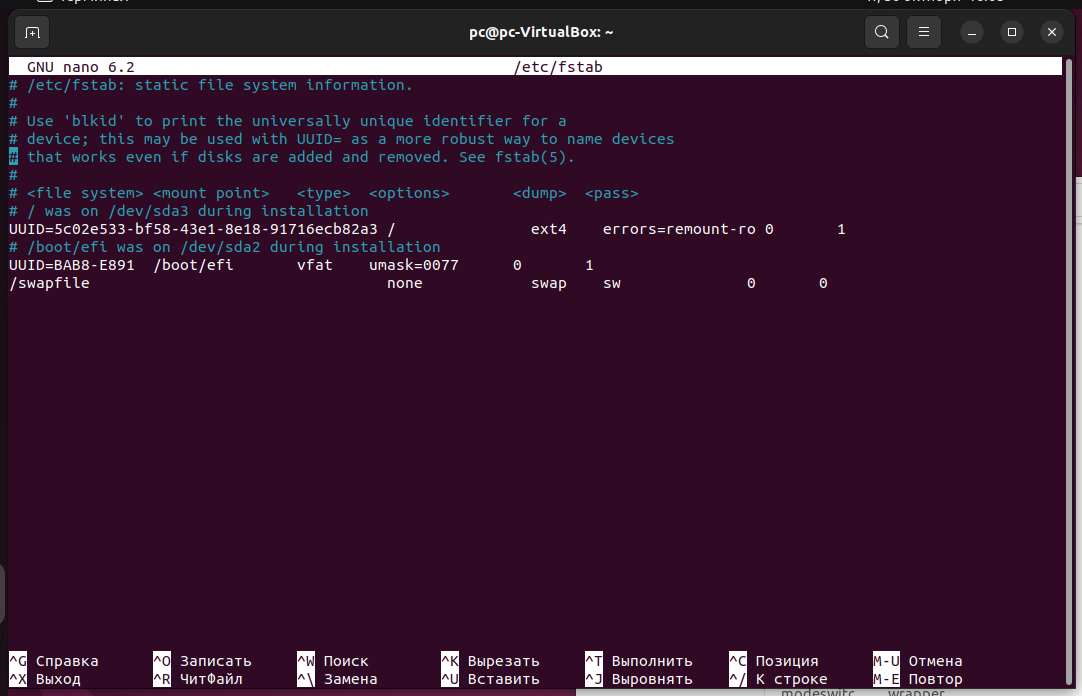


Рисунок 1.3 – папка fsnab через терминал

* 1. Введем в конец файла команду. После чего сохраним файл.



Рисунок 1.4 – ввод команды в терминал

1. 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

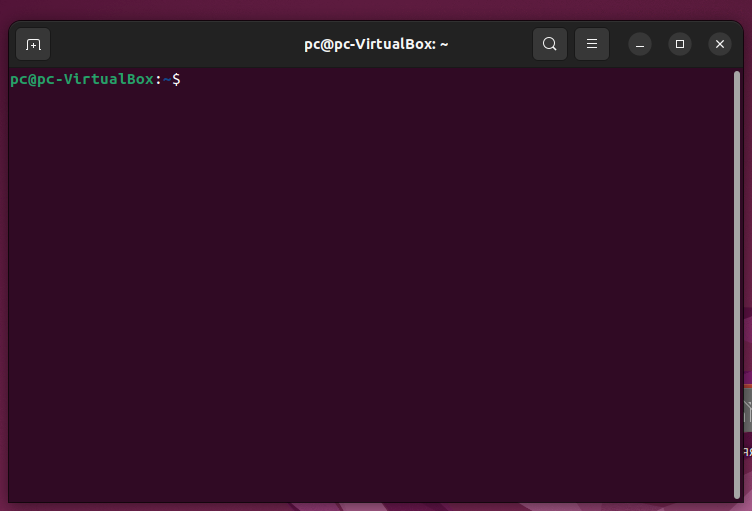


Рисунок 2.1 – окно терминала

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.

1. 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.

* 1. Открываем терминал и вводим команду  sudo apt install gufw.

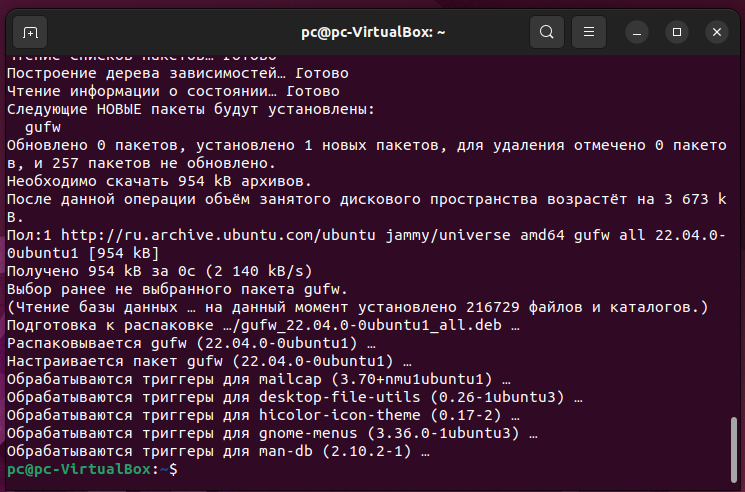


Рисунок 3.1.1 – успешная установка gufw

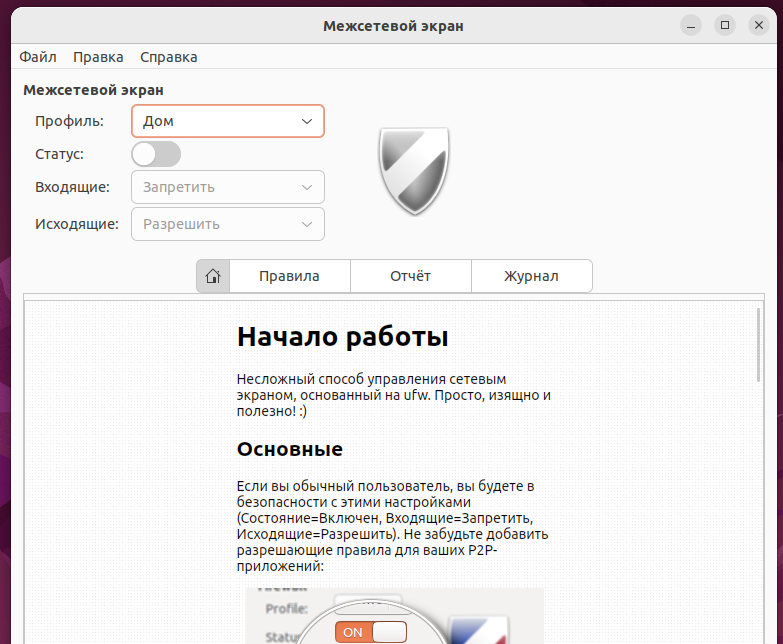


Рисунок 3.1.2 – главное окно gufw

* 1. Включить ограничение входящего и исходящего трафика.

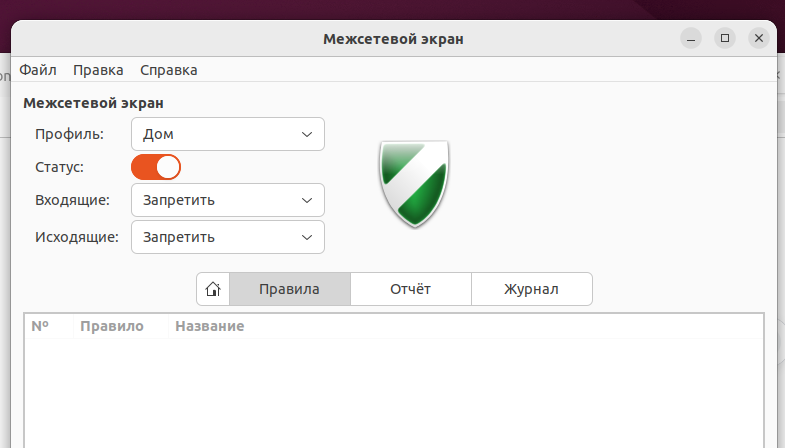


Рисунок 3.2 – включенный режим защиты

* 1. Проверим доступ через команду ping.

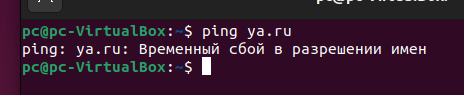


Рисунок 3.3.1 – команда ping

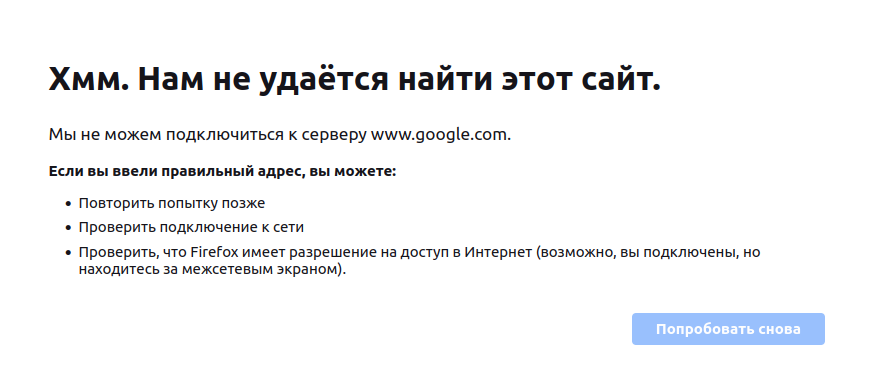


Рисунок 3.3.2 – нет доступа к сети

* 1. Добавим правило для доступа к DNS.

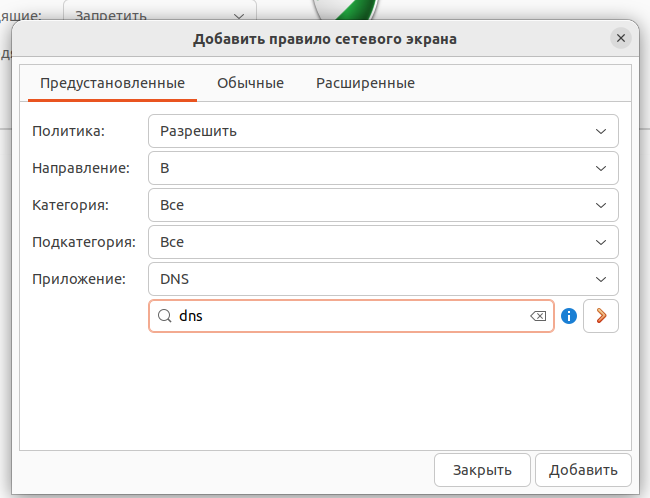


Рисунок 3.4 – добавление правила доступа к DNS

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

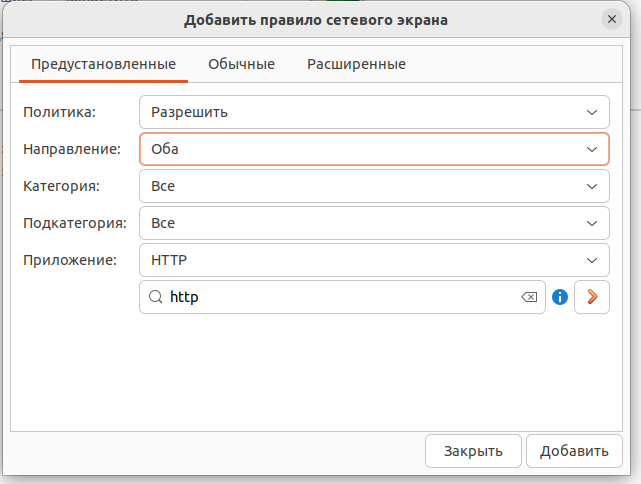


Рисунок 3.5.1 – добавление правила доступа по http

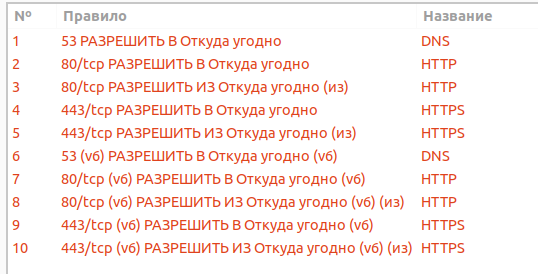


Рисунок 3.5.2 – созданный набор правил

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.