РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №7

дисциплина: Администрирование сетевых подсистем

Студент: Пакавира Арсениу Висенте Луиш

Студ. билет № 1032225105

Группа: НФИбд-02-23

МОСКВА
2025 г.

Цель работы:

Целью данной работы является получение навыков настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

Выполнение работы:

На основе существующего файла описания службы ssh создадим файл с собственным описанием: cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml cd /etc/firewalld/services/

Теперь посмотрим содержимое файла службы (Рис. 1.1):

cat /etc/firewalld/services/ssh-custom.xml

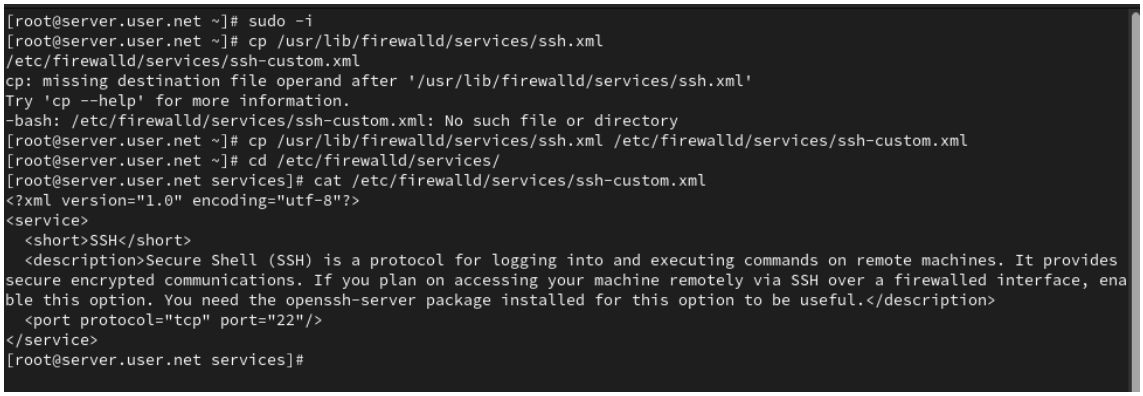


Рис. 1.1. Создание файла с собственным описанием на основе существующего файла описания службы ssh. Просмотр содержимого файла службы.

Откроем файл описания службы на редактирование и заменим порт 22 на новый порт (2022). В этом же файле скорректируем описание службы для демонстрации, что это модифицированный файл службы (Рис. 1.2):

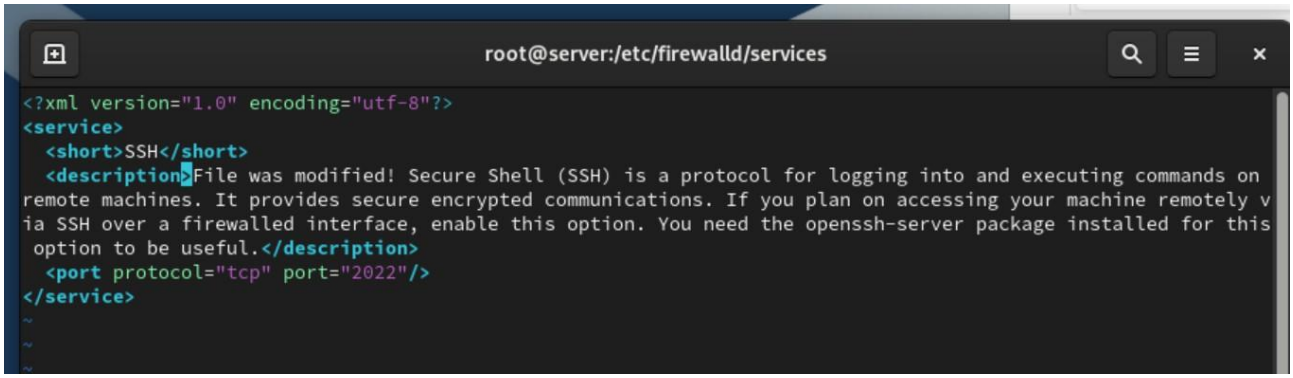


Рис. 1.2. Открытие файла описания службы на редактирование и замена порта 22 на новый порт (2022), корректирование описания службы для демонстрации, что это модифицированный файл службы.

Просмотрим список доступных FirewallD служб (Рис. 1.3):

firewall-cmd --get-services

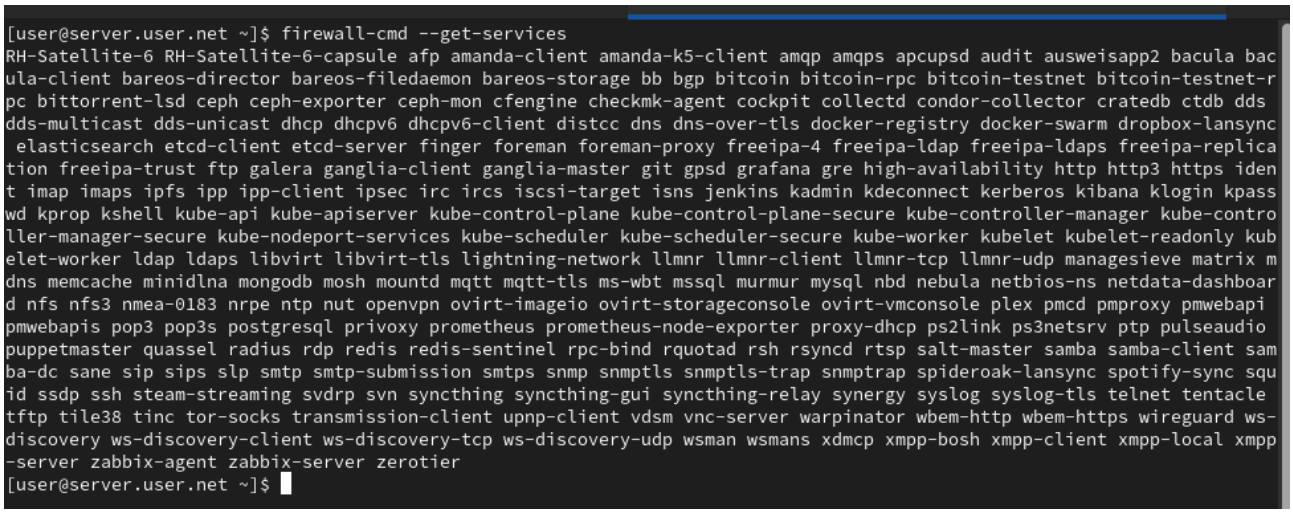


Рис. 1.3. Просмотр списка доступных FirewallD служб.

Перегрузим правила межсетевого экрана с сохранением информации о состоянии и вновь выведем на экран список служб, а также список активных служб:

firewall-cmd --reload
firewall-cmd --get-services firewall-cmd

--list-services

Убедимся, что созданная нами служба отображается в списке доступных для FirewallD служб, но не активирована (Рис. 1.4):

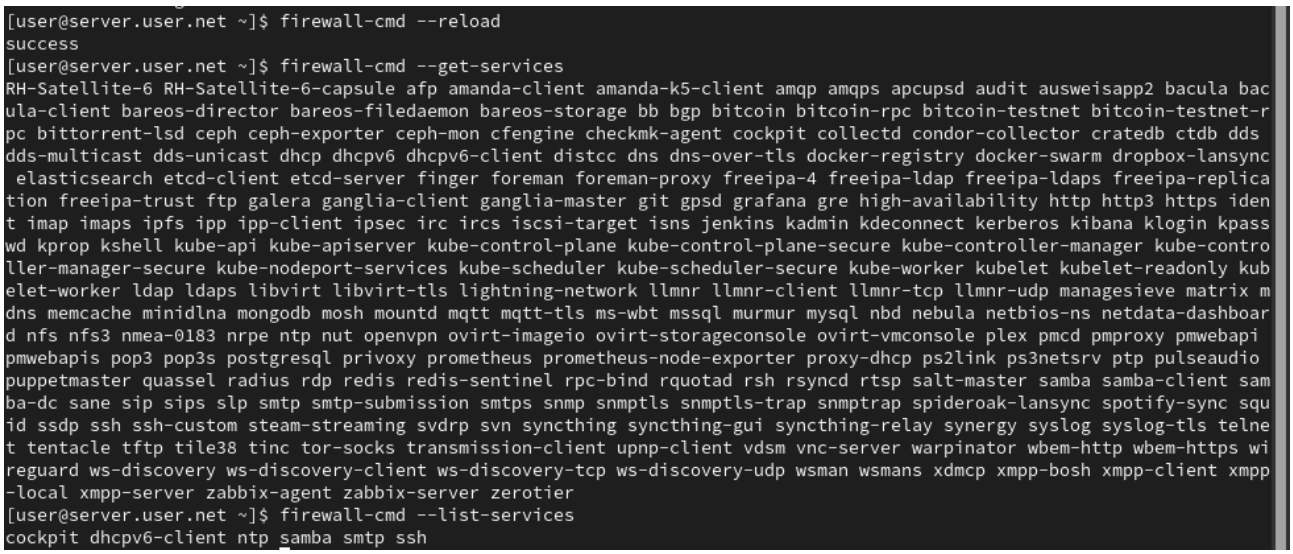


Рис. 1.4. Перегрузка правил межсетевого экрана с сохранением информации о состоянии, вывод на экран списка служб, а также списка активных служб.

Добавим новую службу в FirewallD и выведем на экран список активных служб (Рис. 1.5):

firewall-cmd --add-service=ssh-custom

firewall-cmd --list-services

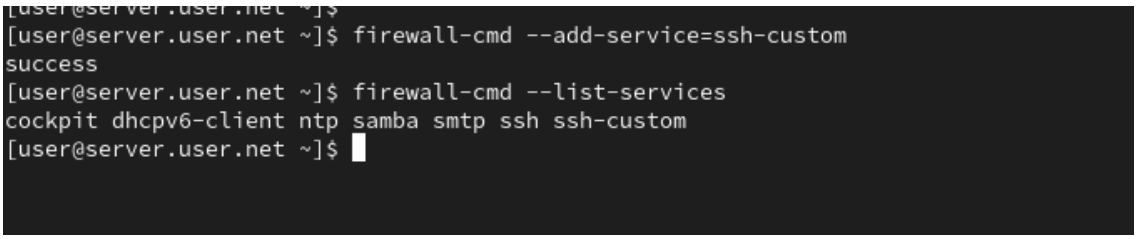


Рис. 1.5. Добавление новой службы в FirewallD и вывод на экран списка активных служб.

Организуем на сервере переадресацию с порта 2022 на порт 22 (Рис. 2.1):

firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22

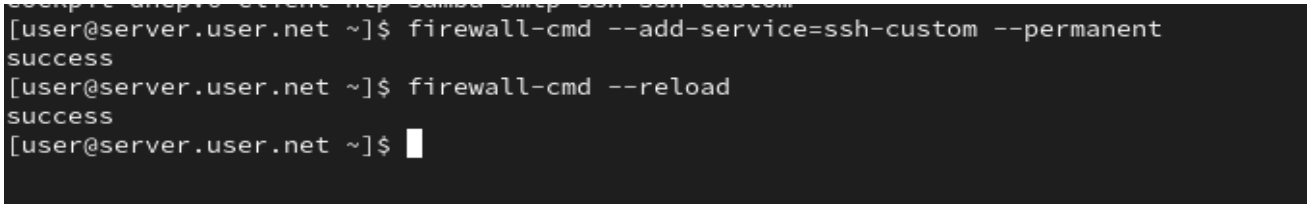


Рис. 2.1. Организация переадресации на сервере с порта 2022 на порт 22.

На клиенте попробуем получить доступ по SSH к серверу через порт 2022 (Рис. 2.2):

ssh -p 2022 user@server.user.net

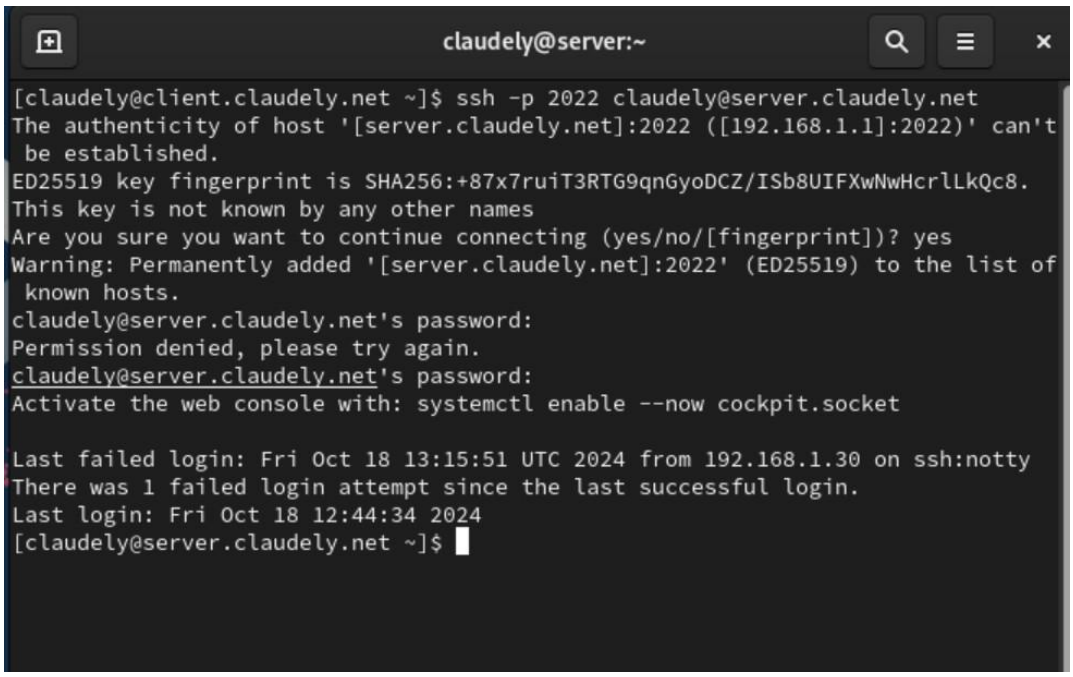


Рис. 2.2. Попытка получить на клиенте доступ по SSH к серверу через порт 2022.

На сервере посмотрим, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов (Рис. 3.1):

sysctl -a | grep forward

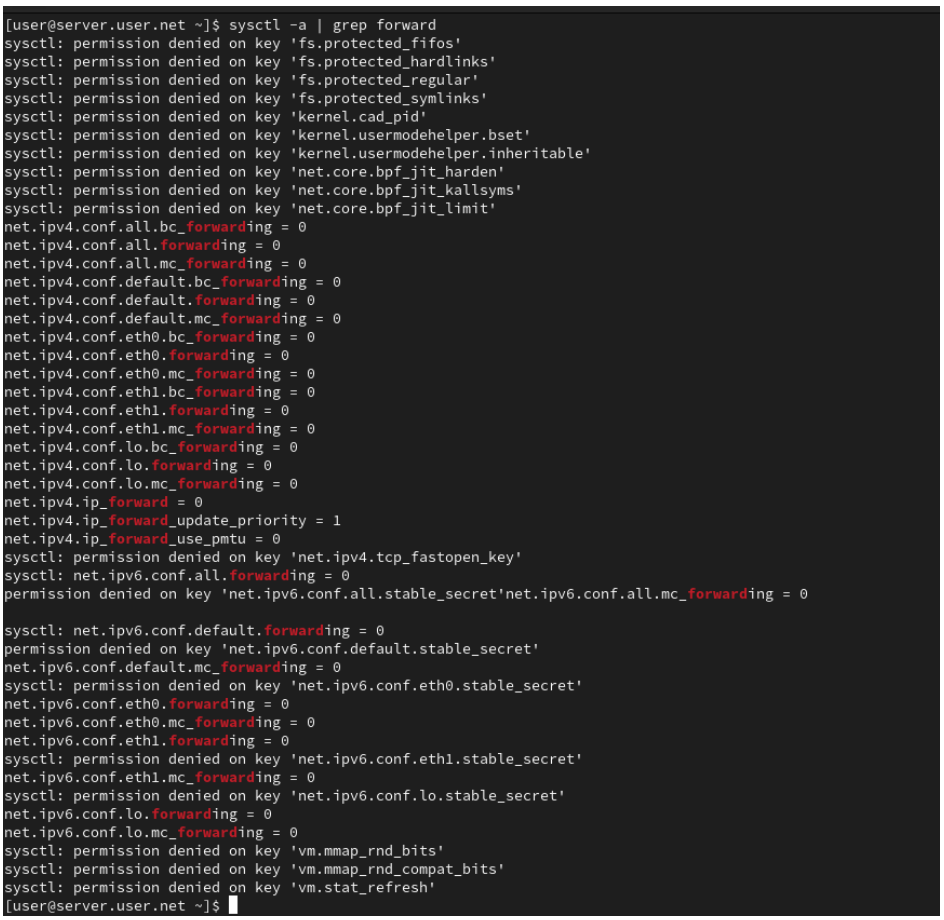


Рис. 3.1. Просмотр на сервере, активирована ли в ядре системы возможность перенаправления IPv4-пакетов.

Включим перенаправление IPv4-пакетов на сервере:

echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf sysctl -p /etc/sysctl.d/90-forward.conf

Затем включим маскарадинг на сервере (Рис. 3.2): firewall-cmd --zone=public --add-masquerade --permanent

firewall-cmd --reload

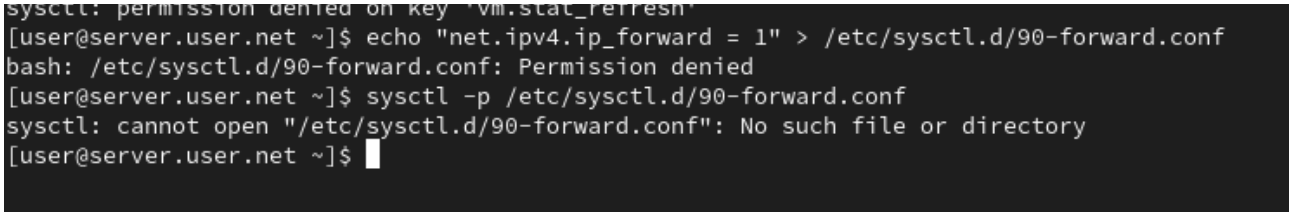


Рис. 3.2. Включение перенаправления IPv4-пакетов на сервере и маскарадинга на сервере.

На клиенте проверим доступность выхода в Интернет (Рис. 3.3):

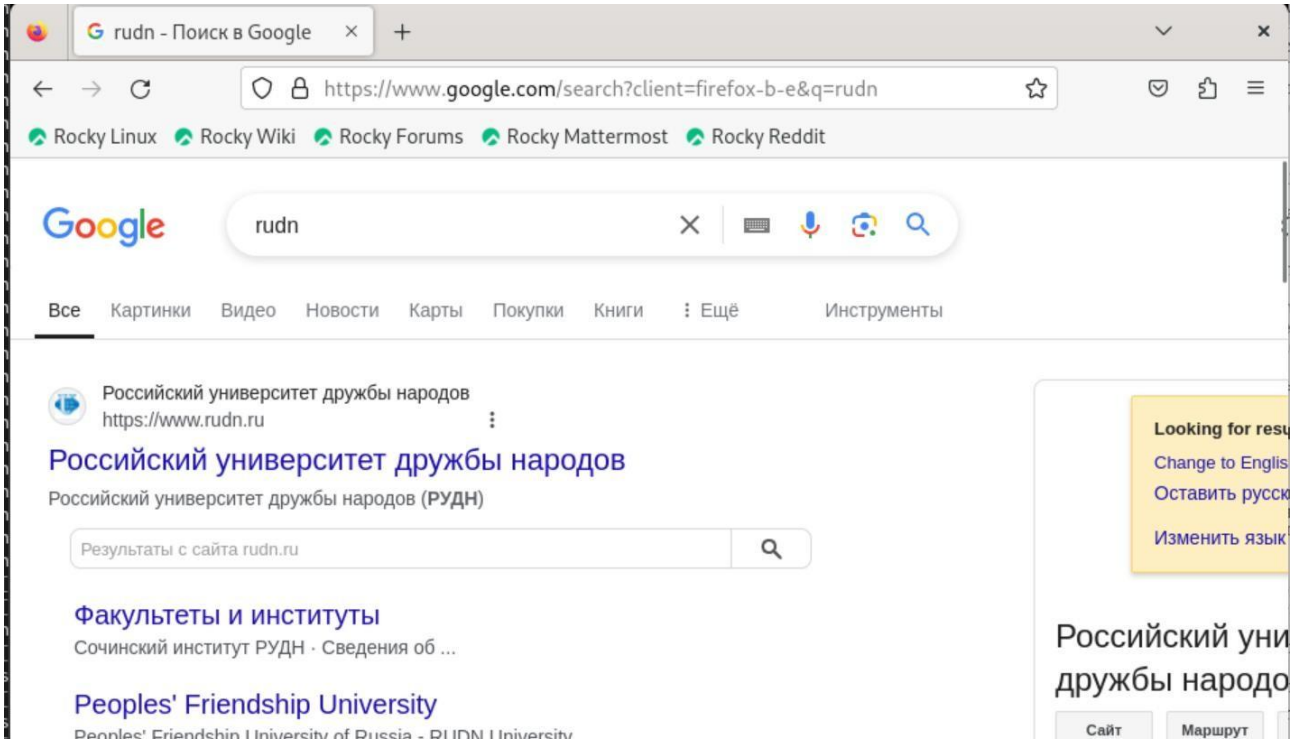
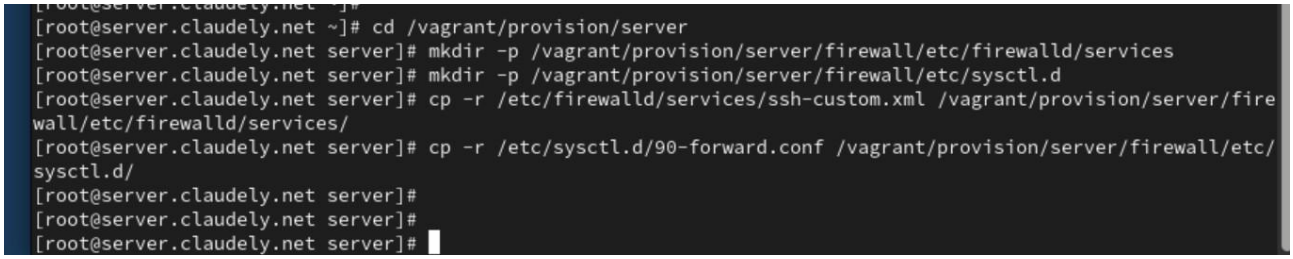


Рис. 3.3. Проверка доступности выхода в Интернет на клиенте.

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог firewall, в который поместим в соответствующие подкаталоги конфигурационные файлы FirewallD. В каталоге /vagrant/provision/server создадим файл firewall.sh (рис. 4.1):



```
[user@server.user.net server]$ cd /vagrant/provision/server
[user@server.user.net server]$ touch firewall.sh
[user@server.user.net server]$ chmod +x firewall.sh
[user@server.user.net server]$
```

Рис. 4.1. Открытие каталога для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога firewall, в который помещаем в соответствующие подкаталоги конфигурационные файлы FirewallD. Создание в каталоге /vagrant/provision/server файла firewall.sh.

Открыв его на редактирование, пропишем в нём следующий скрипт из лабораторной работы (рис. 4.2):

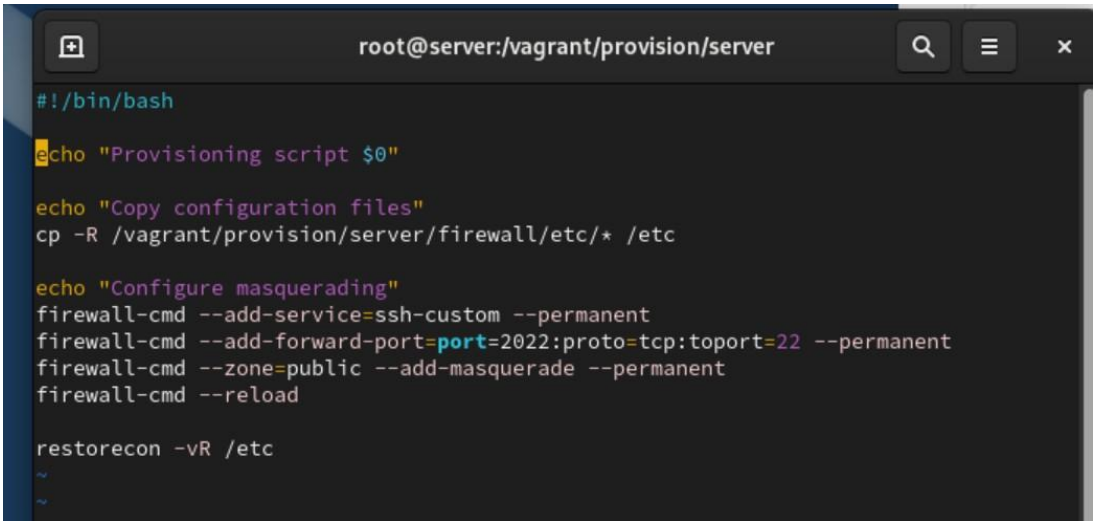


Рис. 4.2. Открытие файла на редактирование и прописывание в нём скрипта из лабораторной работы.

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавим в разделе конфигурации для сервера (рис. 4.3):

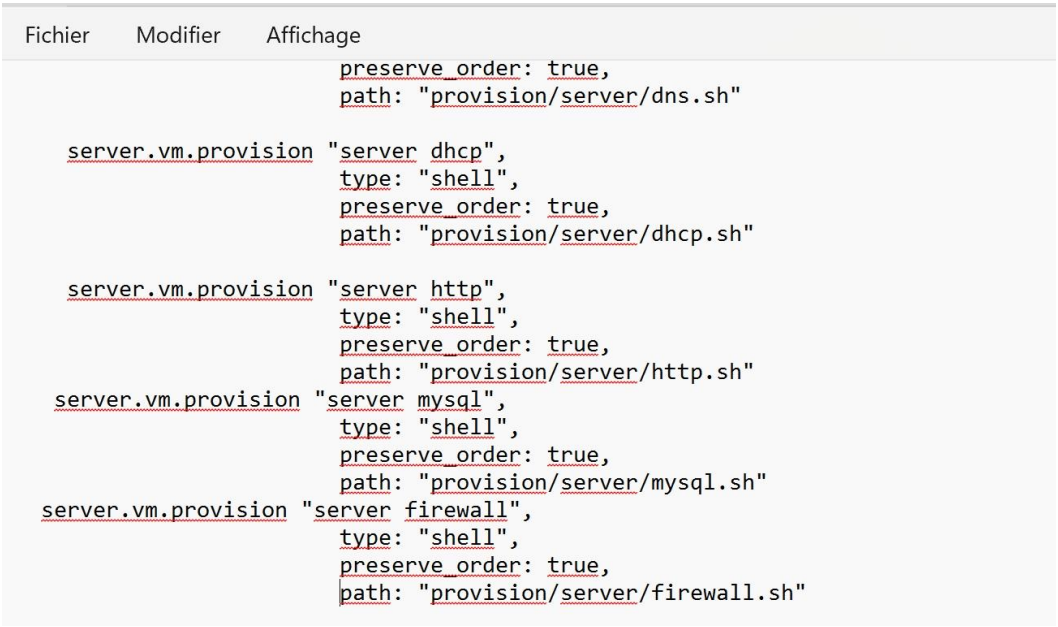


Рис. 4.3. Добавление записи в конфигурационном файле Vagrantfile.

Вывод:

В ходе выполнения лабораторной работы были получены навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

Ответы на контрольные вопросы:

1. Где хранятся пользовательские файлы firewalld? - **В firewalld пользовательские файлы хранятся в директории /etc/firewalld/.**
2. Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022? - **Для указания порта TCP 2022 в пользовательском файле службы, вы можете добавить строку в секцию port следующим образом:**

   <port protocol="tcp" port="2022"/>

3. Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере? - **Чтобы перечислить все службы, доступные в настоящее время на сервере с использованием firewalld, используйте команду: firewall-cmd --get-services**

4. В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)? - **Разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading) заключается в том, что в случае NAT исходный IP-адрес пакета заменяется на IP-адрес маршрутизатора, а в случае маскарадинга используется IP-адрес интерфейса маршрутизатора.**

5. Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10? - **Для разрешения входящего трафика на порт 4404 и перенаправления его на службу SSH по IP-адресу 10.0.0.10, вы можете использовать команды:**

   firewall-cmd --zone=public --add-port=4404/tcp --permanent

   firewall-cmd --zone=public --add-forwardport=port=4404:proto=tcp:toport=22:toaddr=10.0.0.10 -permanent firewall-cmd --reload

6. Какая команда используется для включения маскарадинга IPпакетов для всех пакетов, выходящих в зону public? - **Для включения маскарадинга IP-пакетов для всех пакетов, выходящих в зону public, используйте следующую команду:**

firewall-cmd --zone=public --add-masquerade --permanent

firewall-cmd --reload