Лабораторная работа №7

Шубина София Антоновна

Содержание

# 1 Цель работы

Получить навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

# 2 Задание

1. Настроить межсетевой экран виртуальной машины server для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022.
2. Настроить Port Forwarding на виртуальной машине server.
3. Настроить маскарадинг на виртуальной машине server для организации доступа клиента к сети Интернет.
4. Написать скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внести изменения в Vagrantfile.

# 3 Выполнение лабораторной работы

## 3.1 Создание пользовательской службы firewalld

Перейдем в режим суперпользователя

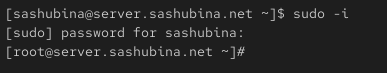


Рис. 1: sudo -i

На основе существующего файла описания службы ssh создадим файл с собственным описанием и посмотрим содержимое файла службы.

Создание файла с собственным описанием

Рис. 2: Создание файла с собственным описанием

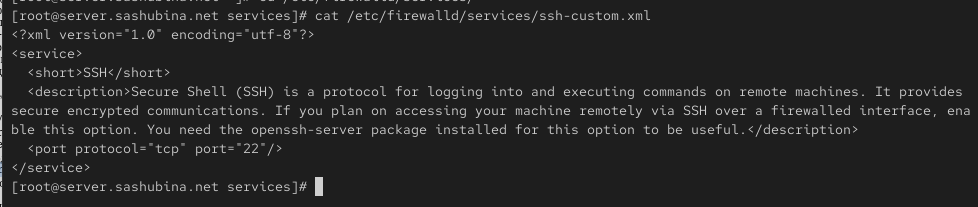


Рис. 3: посмотр файла

В первой строчке указана версия xml и используемая кодировка - utf8. На второй строчке указан тег service, далее его тег-потомок short, внутри которого указан SSH. Затем указан тег description, внутри которого прописано описание протокола ssh, и указан протокол передачи порта tcp и номер порта.

Откроем файл описания службы на редактирование и заменим порт 22 на новый порт (2022):

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

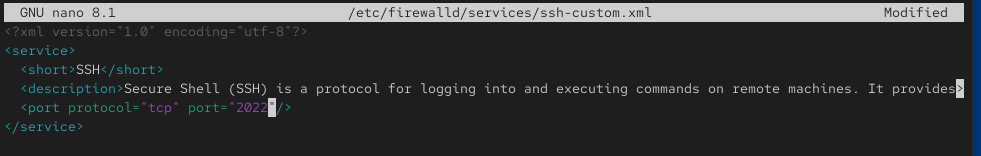


Рис. 4: просмотр файла

В этом же файле скорректируем описание службы для демонстрации, что это модифицированный файл службы.

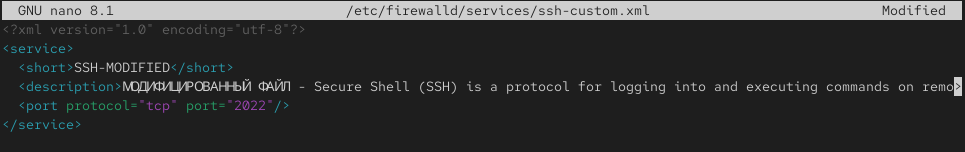


Рис. 5: Отредактированный файл описания службы

Просмотрим список доступных FirewallD служб:

firewall-cmd --get-services

Новая служба ещё не отображается в списке.

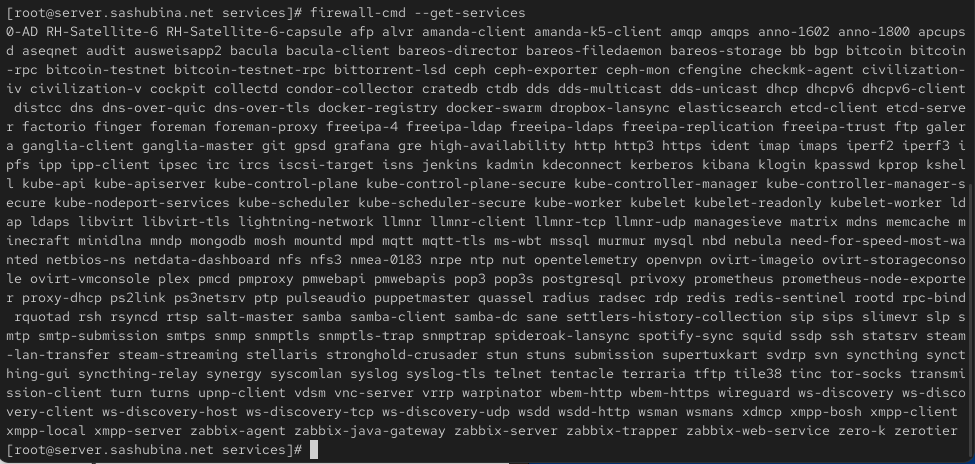


Рис. 6: Список доступных FirewallD служб

Перегрузим правила межсетевого экрана с сохранением информации о состоянии и вновь выведем на экран список служб, а также список активных служб. Созданная служба отображается в списке доступных для FirewallD служб, но не активирована. Добавим новую службу в FirewallD и выведем на экран список активных служб:

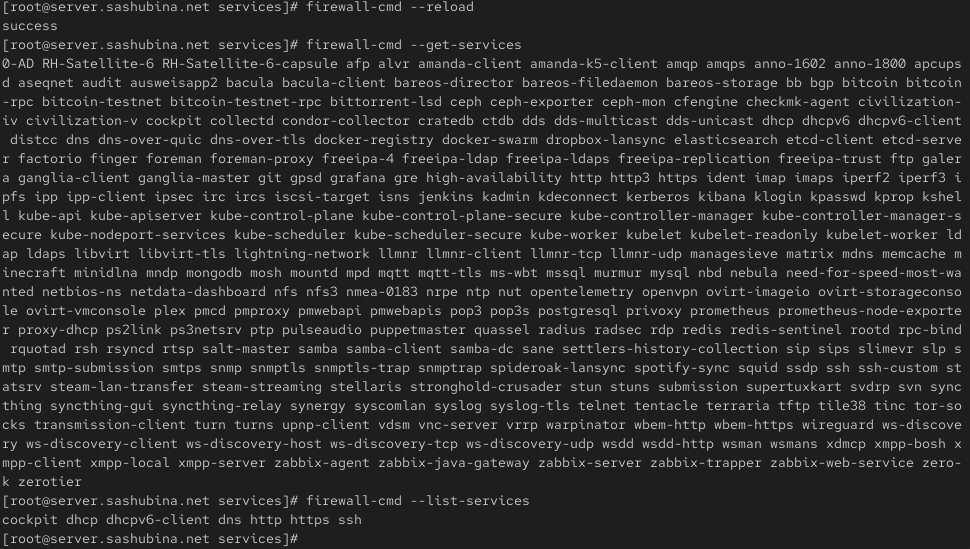


Рис. 7: Список FirewallD служб и добавление новой службы в FirewallD

Организуем на сервере переадресацию с порта 2022 на порт 22:

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

с порта 2022 на порт 22

Рис. 8: с порта 2022 на порт 22

На клиенте попробуем получить доступ по SSH к серверу через порт 2022:

ssh -p 2022 sashubina@server.sashubina.net

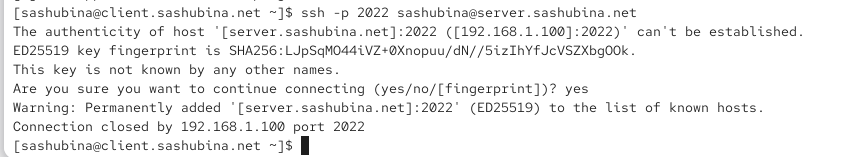


Рис. 9: Переадресация и получение доступа по SSh

## 3.2 Настройка Port Forwarding и Masquerading

На сервере посмотрим, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов:

sysctl -a | grep forward

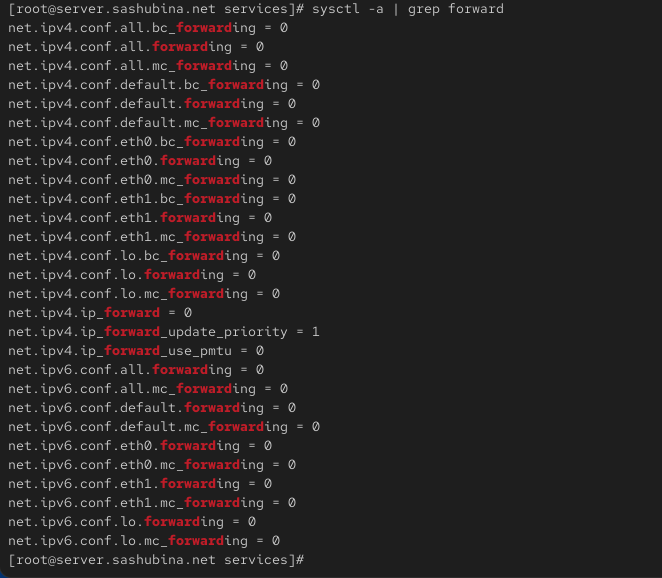


Рис. 10: Проверка активации перенаправления IPv4-пакетов

Возможность не активирована

Включим перенаправление IPv4-пакетов на сервере. Включим маскарадинг на сервере и перезапустим систему:

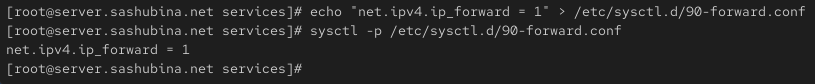


Рис. 11: Включение перенаправление IPv4-пакетов и маскарадинга на сервере

Включим маскарадинг на сервере:

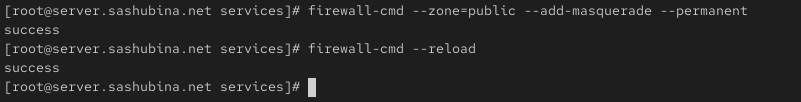


Рис. 12: firewall-cmd–zone=public–add-masquerade–permanent иfirewall-cmd–reload

На клиенте проверим доступность выхода в Интернет.

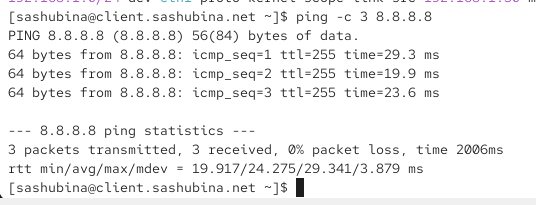


Рис. 13: Проверка доступности выхода в Интернет

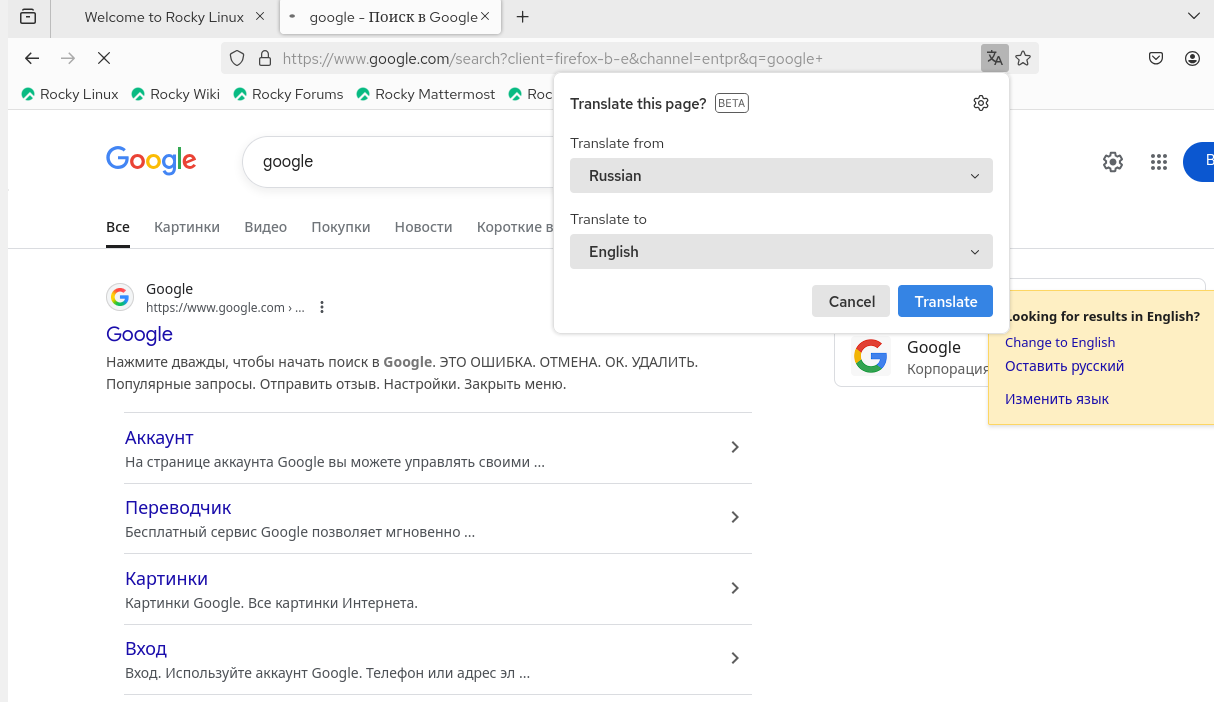


Рис. 14: Проверка доступности выхода в Интернет

Выход в Интернет на клиенте доступен.

## 3.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем 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. 15: Внесения изменений в настройки внутреннего окружения

Внесения изменений в настройки внутреннего окружения

Рис. 16: Внесения изменений в настройки внутреннего окружения

Открыв его на редактирование, пропишите в нём следующий скрипт:

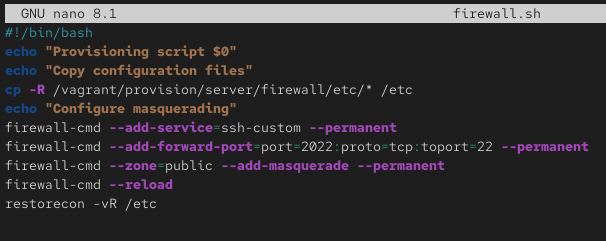


Рис. 17: Редактирование файла

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера:

server.vm.provision "server firewall",  
 type: "shell",  
 preserve\_order: true,  
 path: "provision/server/firewall.sh"

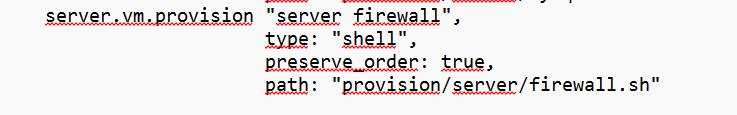


Рис. 18: Редактирование файла

# 4 Выводы

В процессе выполнения данной лабораторной работы я получила навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

# 5 Контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?

/usr/lib/firewalld/services

1. Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?

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

1. Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере?

firewall-cmd --get-services

1. В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)?

При маскарадинге вместо адреса отправителя(как делается это в NAT) динамически подставляется адрес назначенного интерфейса (сетевой адрес + порт).

1. Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10?

sudo firewall-cmd --add-forward-port=port=4404:proto=tcp:toport=22:toaddr=10.0.0.10

1. Какая команда используется для включения маcкарадинга IP-пакетов для всех пакетов, выходящих в зону public?

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