РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 7

**Расширенные настройки межсетевого экрана**

Дисциплина: Администрирование сетевых подсистем

Студент: Карташова А.С.

Группа: НФИбд-03-18

**МОСКВА**

2020 г.

**Оглавление**

[Цель работы 2](#_Toc57950618)

[Задачи 2](#_Toc57950619)

[Ход работы 3](#_Toc57950620)

[Создание пользовательской службы firewalld 3](#_Toc57950621)

[Перенаправление портов 4](#_Toc57950622)

[Настройка Port Forwarding и Masquerading 4](#_Toc57950623)

[Внесение изменений в настройки внутреннего окружения виртуальной машины 6](#_Toc57950624)

[Заключение 7](#_Toc57950625)

[Контрольные вопросы 7](#_Toc57950626)

# Цель работы

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

# Задачи

1. Настроим межсетевой экран виртуальной машины server для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022

2. Настроим Port Forwarding на виртуальной машине server

3. Настроим маскарадинг на виртуальной машине server для организации доступа клиента к сети Интернет

4. Напишем скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внеем изменения в Vagrantfile

# Ход работы

## Создание пользовательской службы firewalld

На основе существующего файла описания службы ssh создадим файл с собственным описанием и посмотрим содержимое файла службы (ssh-custom.xml)

Изображение выглядит как текст

Автоматически созданное описание

***<?xml version="1.0" encoding="utf-8"?> -*** версия докумета и тип шифрования

***<service>***

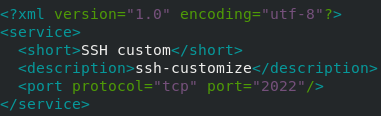
***<short>SSH</short> -*** краткое назвние службы

***<description> description> -*** описание службы

***<port protocol="tcp" port="22"/>-*** номер tcp порта

***</service>***

Откроем файл описания службы на редактирование и заменим порт 22 на новый порт (2022). Скорректируем описание службы для демонстрации, что это модифицированный файл службы.

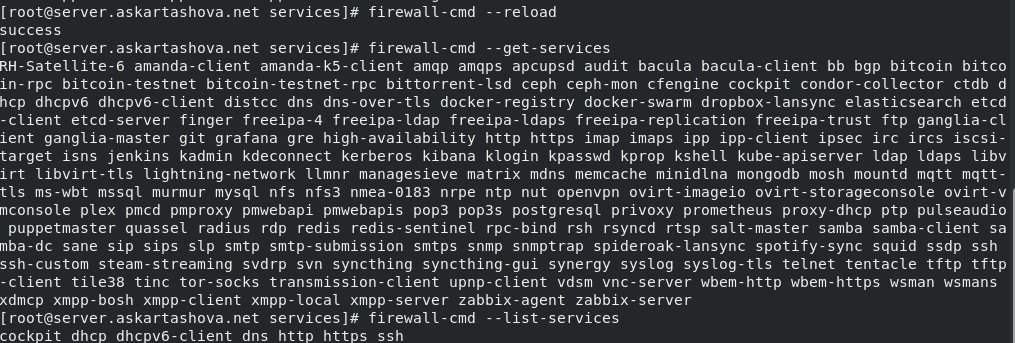


Просмотрим список доступных FirewallD служб. Новой службы в списке нет.

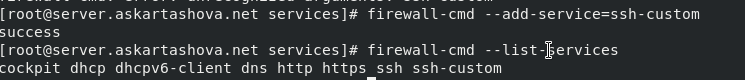
Изображение выглядит как текст

Автоматически созданное описание

Перегрузим правила межсетевого экрана с сохранением информации о состоянии и вновь выведем на экран список служб и список активных служб.Служба отображается в списке доступных, но она не активна.



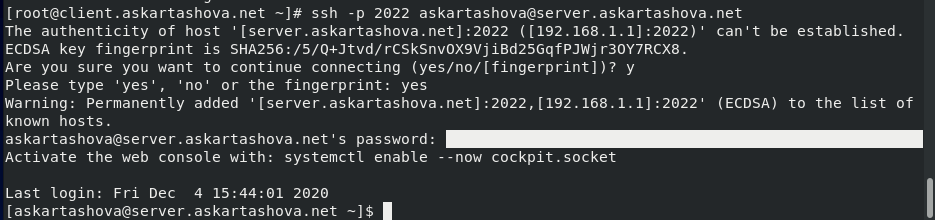
Добавим новую службу в FirewallD и выведем на экран список активных служб



## Перенаправление портов

Организуем на сервере переадресацию с порта 2022 на порт 22

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



## Настройка Port Forwarding и Masquerading

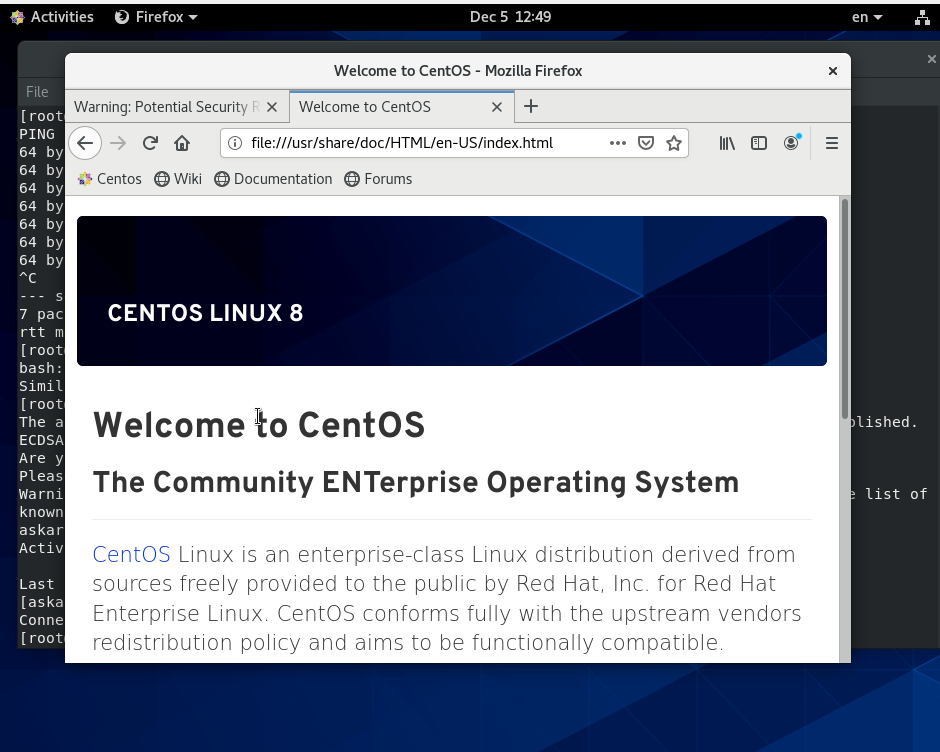
На сервере посмотрим, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов (возможность включена). Включим перенаправление IPv4-пакетов на сервере.

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описаниеВключим маскарадинг на сервере и на клиенте проверим, что выход в интернет доступен.



## 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 исполняемый файл firewall.sh, пропишем в нём следующий скрипт, который повторяет произведённые действия по установке и настройке сервера баз данных.



Изображение выглядит как текст

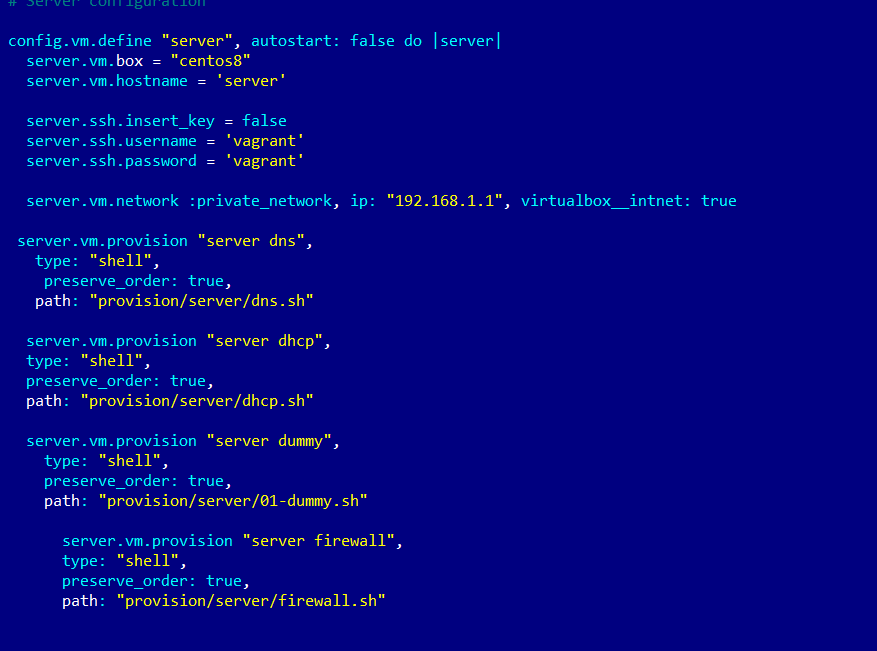
Автоматически созданное описание

Для отработки созданного скрипта во время загрузки виртуальных машин в конфигурационном файле Vagrantfile добавим в конфигурации сервера следующую запись:

*server.vm.provision "server firewall",*

*type: "shell",*

*preserve\_order: true,*

*path: "provision/server/firewall.sh"*

# Заключение

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

# Контрольные вопросы

1.Где хранятся пользовательские файлы firewalld?

Описания хранятся в:

*/usr/lib/firewalld/services/*

Пользовательские файлы хранятся в

*/etc/firewalld/services/*

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

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

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

*firewall-cmd --get-services*

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

(NAT) — механизм преобразования IP-адресов транзитных пакетов. Может производить замену алреса на любой указанный.

Маскарадинг (Masquerading) — тип трансляции сетевого адреса, при которой вместо адреса отправителя динамически подставляется адрес назначенного интерфейса. Использует NAT для замены обратного сетевого адреса пакетов на сетевой адресс шлюза.

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

*firewall-cmd --add-forward-port=port=4404:proto=ssh:toaddr=10.0.0.10*

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

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