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: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

**МОСКВА**

2022 г.

**Цель работы:**

Получить навыки настройки межсетевого экрана в Linux в части переадресации портов

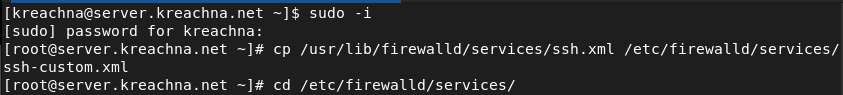
и настройки Masquerading.

**Выполнение работы:**

1. **Создание пользовательской службы firewalld**
2. На основе существующего файла описания службы ssh создайте файл с собственным описанием:

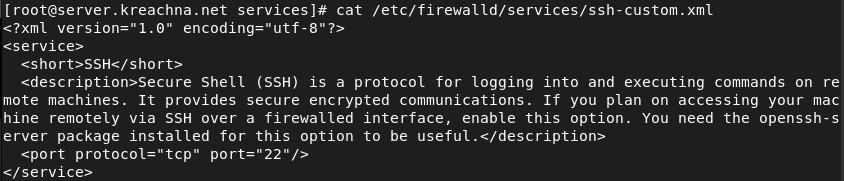
cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml

cd /etc/firewalld/services/

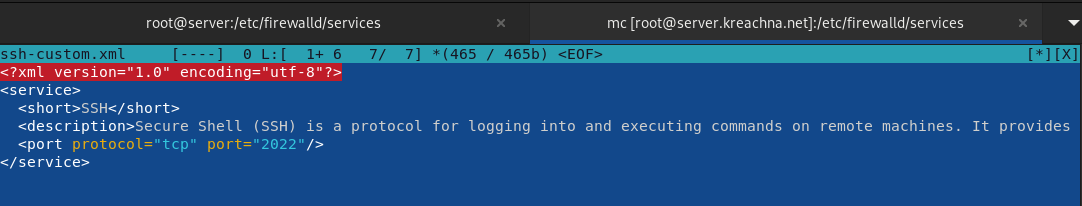


1. Посмотрите содержимое файла службы:

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

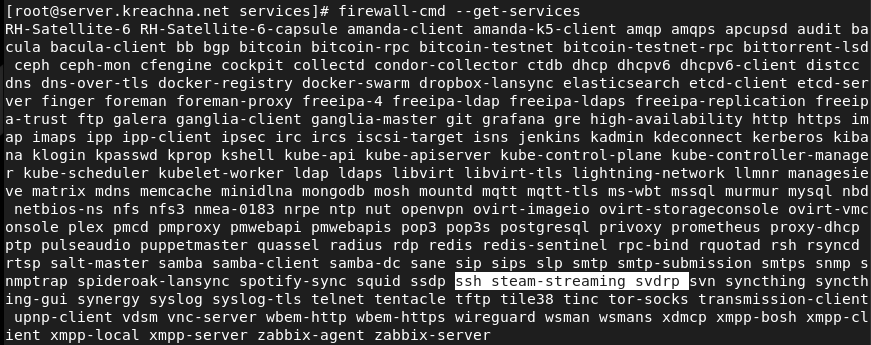


1. Откройте файл описания службы на редактирование и замените порт 22 на новый порт (2022):



1. Просмотрите список доступных FirewallD служб:

firewall-cmd --get-services



1. Перегрузите правила межсетевого экрана с сохранением информации о состоянии и вновь выведите на экран список служб, а также список активных служб:

firewall-cmd --reload

firewall-cmd --get-services

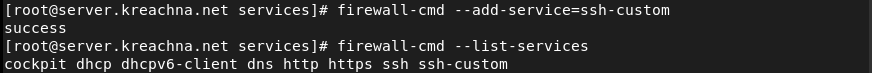
firewall-cmd --list-services



1. Добавьте новую службу в FirewallD и выведите на экран список активных служб:

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

firewall-cmd --list-services



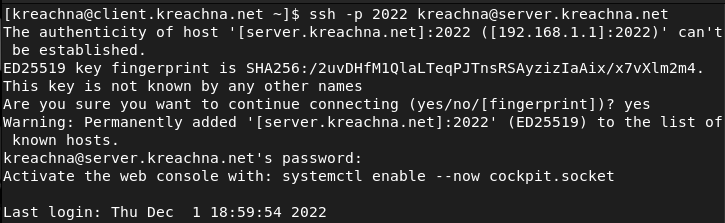
1. **Перенаправление портов**
2. Организуйте на сервере переадресацию с порта 2022 на порт 22:

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



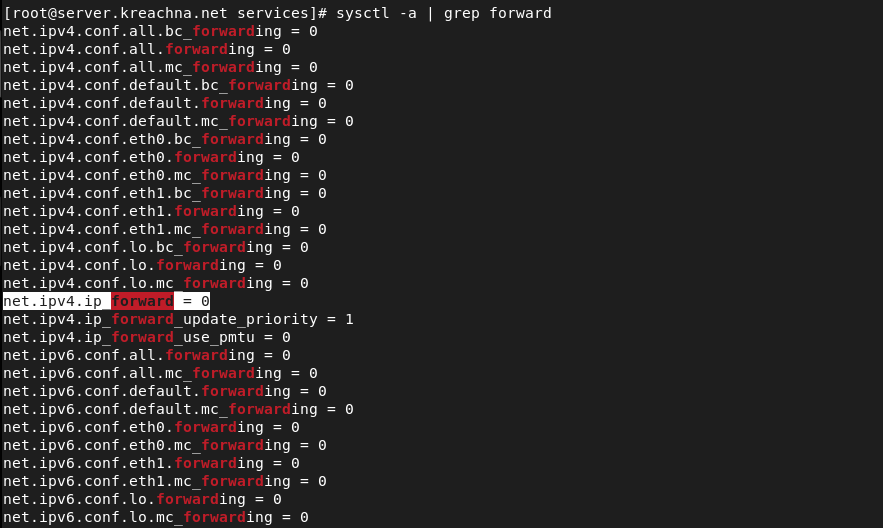
1. На клиенте попробуйте получить доступ по SSH к серверу через порт 2022:

ssh -p 2022 [kreachna@server.kreachna.net](mailto:kreachna@server.kreachna.net)



1. **Настройка Port Forwarding и Masquerading**
2. На сервере посмотрите, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов:

sysctl -a | grep forward



1. Включите перенаправление IPv4-пакетов на сервере:

echo "net.ipv4.ip\_forward = 1" > /etc/sysctl.d/90-forward.conf

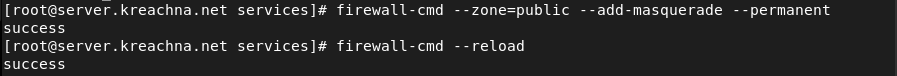
sysctl -p /etc/sysctl.d/90-forward.conf



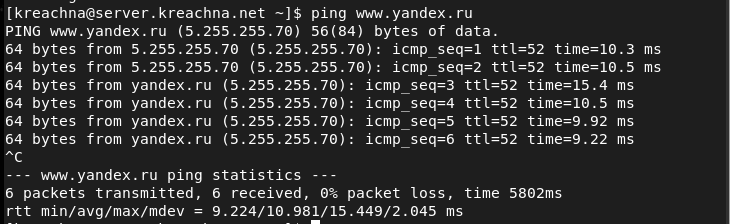
1. Включите маскарадинг на сервере:

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

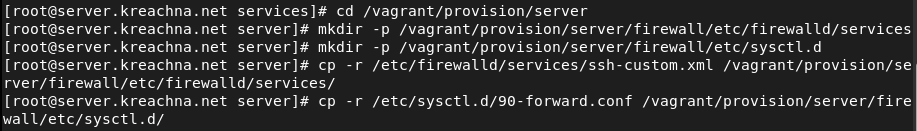
firewall-cmd –reload



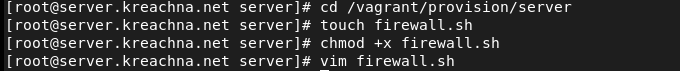
1. На клиенте проверьте доступность выхода в Интернет.



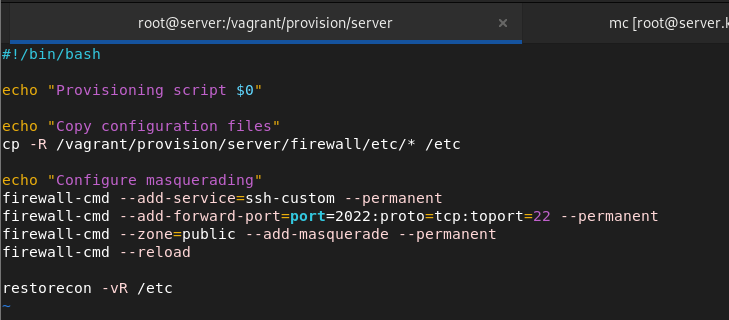
1. **Внесение изменений в настройки внутреннего окружения виртуальной машины**
2. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог firewall, в который поместите в соответствующие подкаталоги конфигурационные файлы FirewallD:



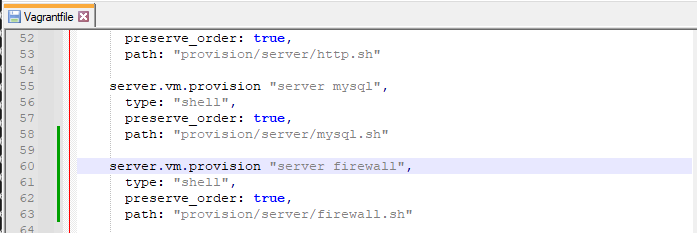
1. В каталоге /vagrant/provision/server создайте файл firewall.sh:



Открыв его на редактирование, пропишите в нём следующий скрипт:



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



**Ответ на контрольные вопрос**

1. Где хранятся пользовательские файлы firewalld?

/usr/lib/firewalld/services/ssh.xml

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)?

NAT производит замену адреса на любой указанный, а маскарадинг только на адрес, машины, выполняющей маскарад.

1. 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

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

firewall-cmd --zone=public --add-masquerad

**Вывод:**

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