Отчет по лабораторной работе №7

Расширенные настройки межсетевого экрана

Галацан Николай, НПИбд-01-22

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

## 2.1 Создание пользовательской службы firewalld

Запускаю ВМ через рабочий каталог. На ВМ server вхожу под собственным пользователем и перехожу в режим суперпользователя. На основе существующего файла описания службы ssh создаю файл с собственным описанием. Просматриваю содержимое файла (рис. 1).

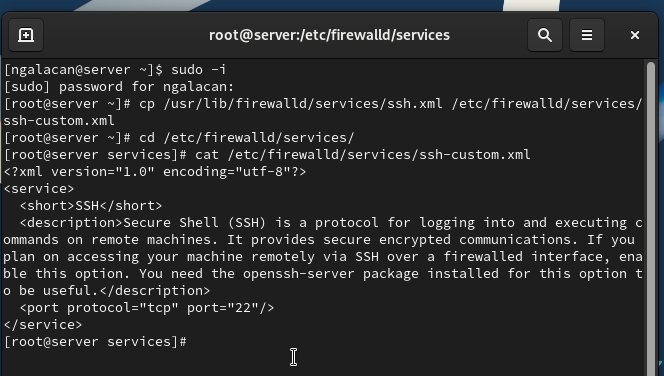


Рис. 1: Создание собственного файла описания службы и просмотр

Открываю файл на редактирование и меняю порт 22 на порт 2022, в описании службы указав, что файл был модифицирован (рис. 2)

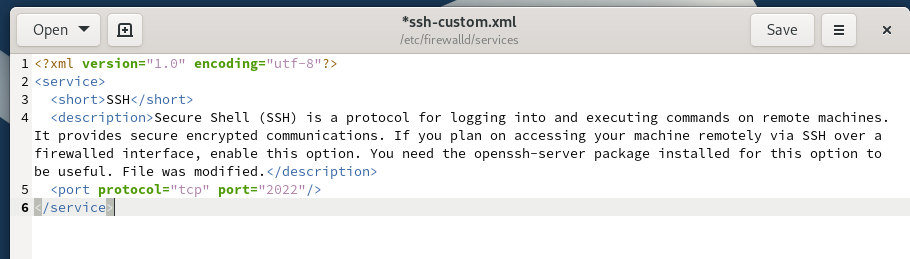


Рис. 2: Редактирование файла описания службы

Просматриваю список доступных служб (новой службы пока нет). Перезагружаю правила межсетевого экрана, снова просматриваю список доступных служб и вижу новую (рис. 3)

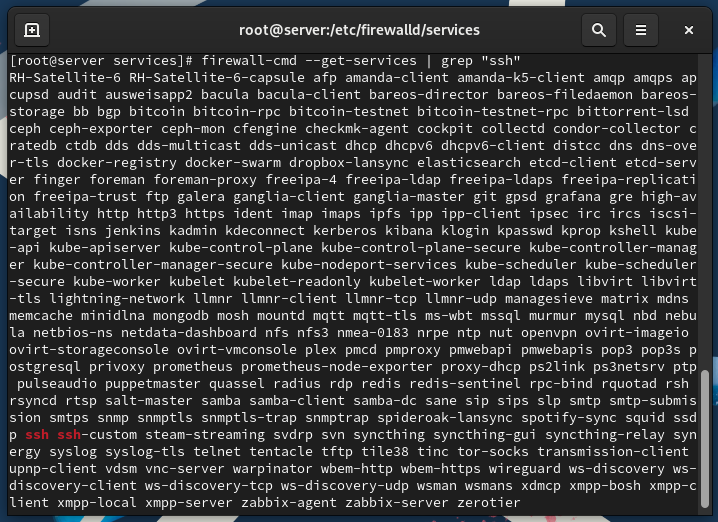


Рис. 3: Новая служба в списке доступных служб

Новая служба отображается в списке доступных, но пока не активирована. Добавляю новую службу в FirewallD и просматриваю список активных служб (служба появилась). Перегружаю правила межсетевого экрана с сохранением информации о состоянии (рис. 4)

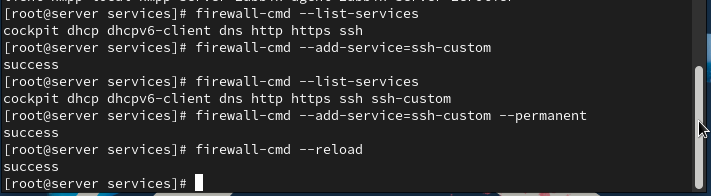


Рис. 4: Добавление новой службы и просмотр списка активных служб, сохранение информации о состоянии

## 2.2 Перенаправление портов

Организовываю переадресацию с порта 2022 на порт 22 на сервере, введя команду

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

На клиенте пробую получить доступ по SSH через порт 2022. Доступ получен (рис. 5).

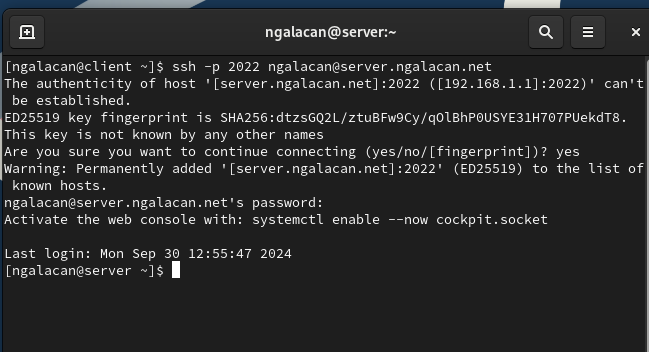


Рис. 5: Доступ по SSH к серверу через порт 2022 на клиенте

## 2.3 Настройка Port Forwarding и Masquerading

На сервере просматриваю, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов. Включаю перенаправление пакетов на сервере. Включаю маскарадинг на сервере (рис. 6). Убеждаюсь, что на клиенте доступен выход в интернет (веб-страницы в браузере загружаются успешно).

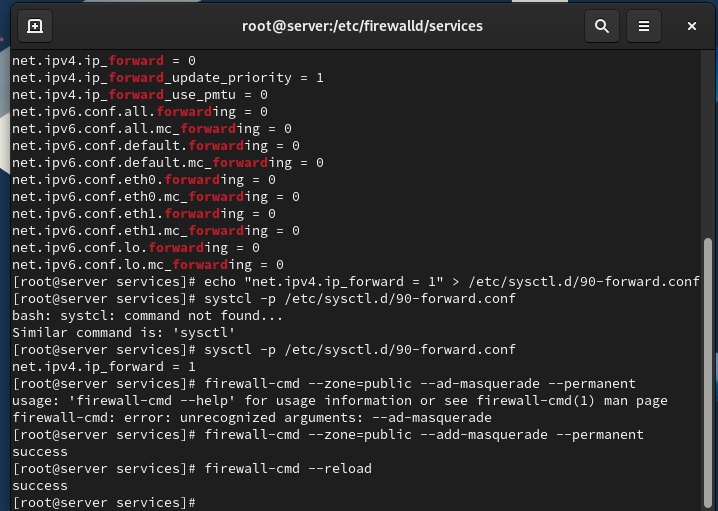


Рис. 6: Включение перенаправления пакетов и включение маскарадинга

## 2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

На ВМ server перехожу в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и копирую в соответствующие каталоги конфигурационные файлы. Создаю скрипт firewall.sh (рис. 7).

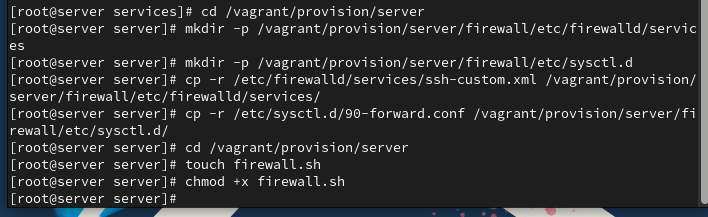


Рис. 7: Создание каталогов и копирование конфигурационных файлов, создание скрипта firewall.sh

Редактирую скрипт (рис. 8).



Рис. 8: Редактирование firewall.sh

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавляю в разделе конфигурации для сервера следующую запись:

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

# 3 Выводы

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

# 4 Ответы на контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?

* В firewalld пользовательские файлы хранятся в директории /etc/firewalld/.

1. 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"/>

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)?

* 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 маршрутизатора.

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

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

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

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