Отчёт по лабораторной работе №7

Дисциплина: Администрирование сетевых подсистем

true

Содержание

Цель работы

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

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

Выполнение лабораторной работы

Создание пользовательской службы firewalld

Загрузили нашу операционную систему и перешли в рабочий каталог с проектом: `cd /var/tmp/tbmanturov/vagrant` ([рис. @fig-001])

Запустили виртуальную машину server: `make server-up` ([рис. @fig-002])

Далее на виртуальной машине server вошли под созданным нами в предыдущей работе пользователем и открыли терминал. Перешли в режим суперпользователя: `sudo -i` ([рис. @fig-003])

Далее на основе существующего файла описания службы ssh создали файл с собственным описанием: `cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml` ([рис. @fig-004])

Создание файла описания службы ssh с собственным описанием

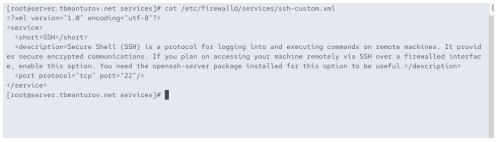
Далее посмотрели содержимое файла службы: `cat /etc/firewalld/services/ssh-custom.xml`([рис. @fig-005])

Пояснения к файлу службы:

- `<?xml ...?>` — объявление XML-документа, версия и кодировка.
- `<service>` — корневой элемент, описывающий службу.
- `<short>` — краткое название службы (например, “SSH”).

- `<description>` — подробное описание назначения службы.
- `<port protocol="..." port="..."/>` — указание протокола и порта службы (здесь TCP/22).

Файл используется для настройки правил firewall (например, в firewalld) для разрешения доступа к службе.

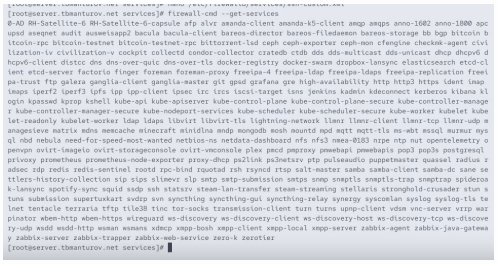


Содержимое файла службы

Далее открыли файл описания службы на редактирование и заменили порт 22 на новый порт (2022): `<port protocol="tcp" port="2022"/>`. В этом же файле скорректировали описание службы, указал что это модифицированный файл службы ([рис. @fig-006])

Редактирование файла описания службы

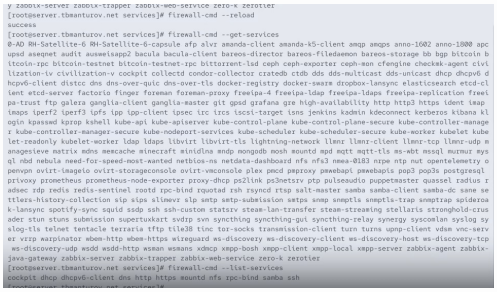
Посмотрели список доступных FirewallD служб: `firewall-cmd --get-services` ([рис. @fig-007])



Список доступных FirewallD служб

Далее перезагрузили правила межсетевого экрана с сохранением информации о состоянии и вновь вывели на экран список служб, а также список активных служб ([рис. @fig-008]):

```
firewall-cmd --reload

firewall-cmd --get-services

firewall-cmd --list-services
```



Перезагрузка правил межсетевого экрана с сохранением информации о состоянии, список доступных служб, список активных служб

Добавили новую службу в FirewallD и вывели на экран список активных служб ([рис. @fig-009]):

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

firewall-cmd --list-services
```

Добавление новой службы в FirewallD, список активных служб

Служба успешно добавлена в FirewallD, поэтому мы перезагрузили правила межсетевого экрана с сохранением информации о состоянии ([рис. @fig-010]):

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

firewall-cmd --reload
```

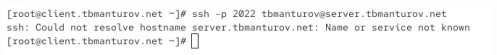
Перезагрузка правил межсетевого экрана с сохранением информации о состоянии

Перенаправление портов

Далее организовли на сервере переадресацию с порта 2022 на порт 22: `firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22` ([рис. @fig-011])

Переадресация с порта 2022 на порт 22

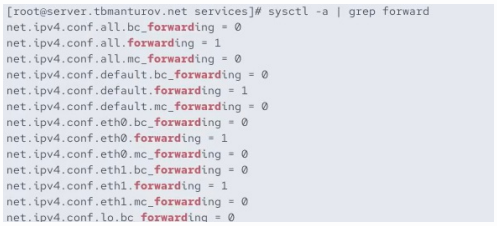
На клиенте попробовали получить доступ по SSH к серверу через порт 2022: `ssh -p 2022 tbmanturov@server.tbmanturov.net` ([рис. @fig-012]), ([рис. @fig-013])



Доступ на клиенте по SSH к серверу через порт 2022

Настройка Port Forwarding и Masquerading

На сервере посмотрели, активирована ли в ядре системы возможность перенаправления IPv4-пакетов: `sysctl -a | grep forward` ([рис. @fig-014])



Проверка возможности перенаправления IPv4-пакетов в ядре системы

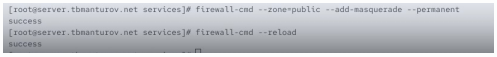
Далее включили перенаправление IPv4-пакетов на сервере ([рис. @fig-015]):

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

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

Включение перенаправления IPv4-пакетов на сервере

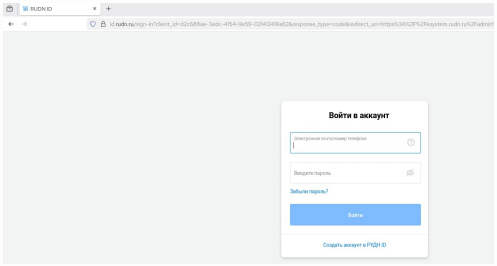
Включили маскарадинг на сервере ([рис. @fig-016]):

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

firewall-cmd --reload
```



Включение маскарадинга на сервере

Далее на клиенте проверили доступность выхода в Интернет ([рис. @fig-017])



Проверка входа в Интернет на клиенте

Внесение изменений в настройки внутреннего окружения виртуальной машины

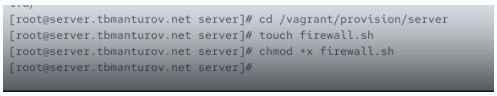
На виртуальной машине server перешли в каталог для внесения изменений в настройки внутреннего окружения */vagrant/provision/server/*, создали в нём каталог *firewall*, в который поместили в соответствующие подкаталоги конфигурационные файлы FirewallD ([рис. @fig-018]):

```
cd /vagrant/provision/server

mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services

mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d

cp -r /etc/firewalld/services/ssh-custom.xml
/vagrant/provision/server/firewall/etc/firewalld/services/

cp -r /etc/sysctl.d/90-forward.conf
/vagrant/provision/server/firewall/etc/sysctl.d/
```

Копирование конфигурационных файлов в каталог firewall

В каталоге /vagrant/provision/server создали исполняемый файл firewall.sh ([рис. @fig-019]):

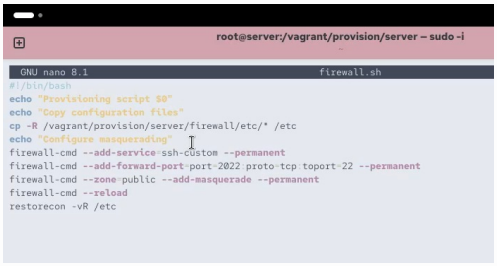
```
cd /vagrant/provision/server

touch firewall.sh

chmod +x firewall.sh
```



Создание исполняемого файла firewall.sh

Открыв его на редактирование прописали в нём следующие строки ([рис. @fig-020]):

```
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/firewall/etc/* /etc
echo "Configure masquerading"
firewall-cmd --add-service=ssh-custom --permanent
firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22 --permanent
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload
restorecon -vR /etc
```

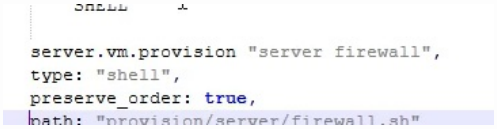


Редактирование файла firewall.sh

Этот скрипт повторяет произведённые нами действия по настройке межсетвеого экрана в части переадресации портов и настройки Masquerading

Для отработки созданного скрипта во время загрузки виртуальных машин в конфигурационном файле Vagrantfile необходимо добавить в конфигурации сервера следующую запись ([рис. @fig-021]):

```
server.vm.provision "server firewall",
    type: "shell",
    preserve_order: true,
    path: "provision/server/firewall.sh""
```



Редактирование Vagrantfile

После этого можно выключать виртуальные машины server и client: `make server-halt` и `make client-halt`([рис. @fig-022])

Контрольные вопросы + ответы

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, можно добавить строку в секцию port следующим образом:

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, используется команда: 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, можно использовать команды:

- 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

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

Для включения маскарадинга IP-пакетов для всех пакетов, выходящих в зону public, можно использовать команды:

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

Выводы

В ходе выполнения лабораторной работы №7 мы получили навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

Список литературы

1. Лабораторая работа №7