

Отчет по лабораторной работе №7

Расширенные настройки межсетевого экрана

Галацан Николай, НПИбд-01-22

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
2.1	Создание пользовательской службы firewalld	5
2.2	Перенаправление портов	7
2.3	Настройка Port Forwarding и Masquerading	7
2.4	Внесение изменений в настройки внутреннего окружения виртуальной машины	8
3	Выводы	10
4	Ответы на контрольные вопросы	11

Список иллюстраций

2.1	Создание собственного файла описания службы и просмотр	5
2.2	Редактирование файла описания службы	6
2.3	Новая служба в списке доступных служб	6
2.4	Добавление новой службы и просмотр списка активных служб, со- хранение информации о состоянии	7
2.5	Доступ по SSH к серверу через порт 2022 на клиенте	7
2.6	Включение перенаправления пакетов и включение маскардинга	8
2.7	Создание каталогов и копирование конфигурационных файлов, со- здание скрипта firewall.sh	8
2.8	Редактирование firewall.sh	9

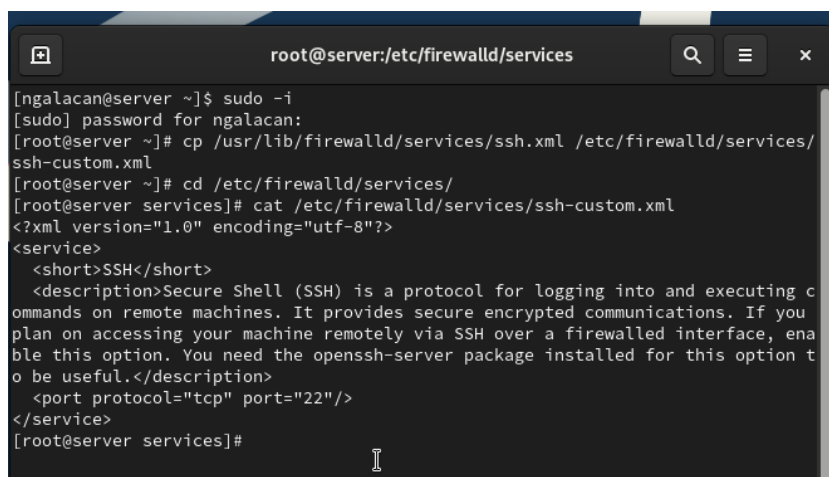
1 Цель работы

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 VM через рабочий каталог. На VM 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. 2.1).



```
root@server:/etc/firewalld/services
[ngalacan@server ~]$ sudo -i
[sudo] password for ngalacan:
[root@server ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server ~]# cd /etc/firewalld/services/
[root@server services]# cat /etc/firewalld/services/ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing c
ommands on remote machines. It provides secure encrypted communications. If you
plan on accessing your machine remotely via SSH over a firewalled interface, ena
ble this option. You need the openssh-server package installed for this option t
o be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server services]#
```

Рис. 2.1: 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. 2.2)



Рис. 2.2: Редактирование файла описания службы

Просматриваю список доступных служб (новой службы пока нет). Перегружаю правила межсетевого экрана, снова просматриваю список доступных служб и вижу новую (рис. 2.3)

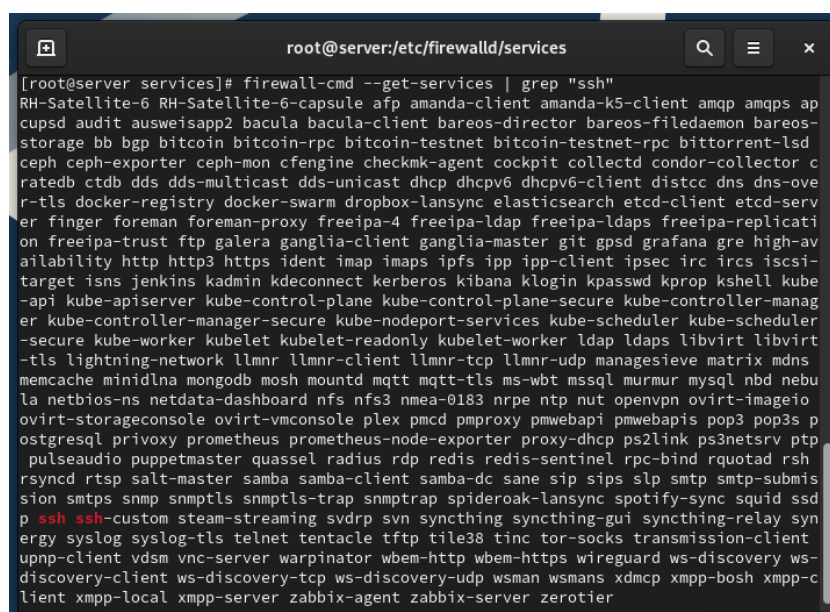


Рис. 2.3: Новая служба в списке доступных служб

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. 2.4)

```
[root@server services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server services]# firewall-cmd --add-service=ssh-custom
success
[root@server services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server services]# firewall-cmd --reload
success
[root@server services]#
```

Рис. 2.4: 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. 2.5).

```
ngalacan@server:~
[ngalacan@client ~]$ ssh -p 2022 ngalacan@server.ngalacan.net
The authenticity of host '[server.ngalacan.net]:2022 ([192.168.1.1]:2022)' can't
be established.
ED25519 key fingerprint is SHA256:dtzsGQ2L/ztuBFw9Cy/q0lBhP0USYE31H707PUekdT8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[server.ngalacan.net]:2022' (ED25519) to the list of
known hosts.
ngalacan@server.ngalacan.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

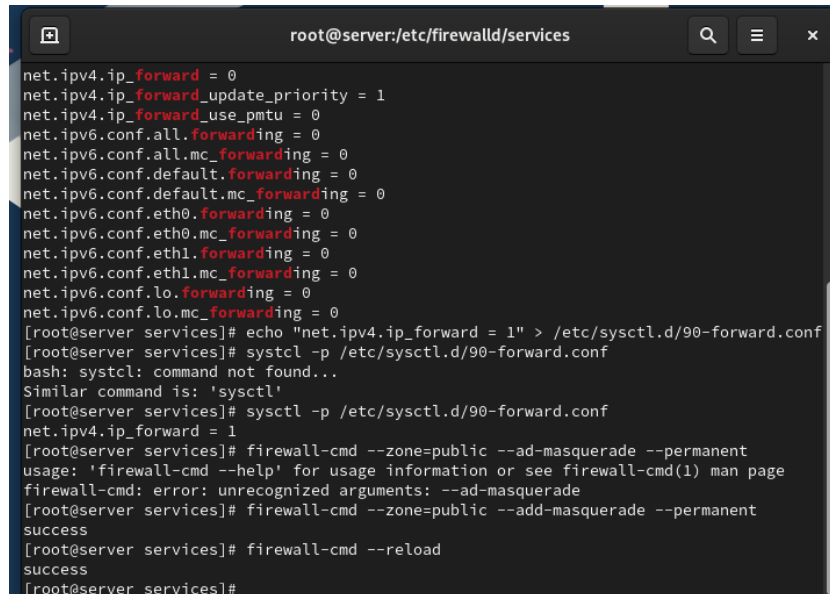
Last login: Mon Sep 30 12:55:47 2024
[ngalacan@server ~]$
```

Рис. 2.5: 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. Включаю перенаправление пакетов на

сервере. Включаю маскарading на сервере (рис. 2.6). Убеждаюсь, что на клиенте доступен выход в интернет (веб-страницы в браузере загружаются успешно).

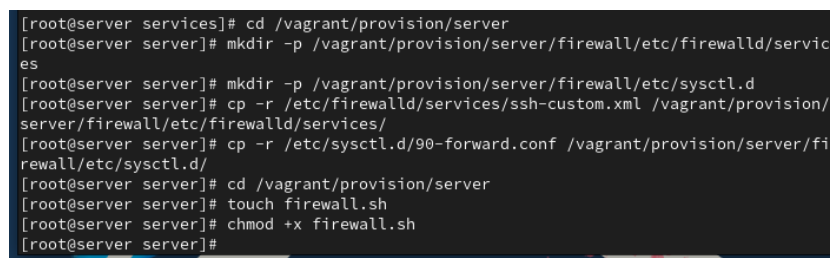


```
root@server:/etc/firewalld/services
net.ipv4.ip_forward = 0
net.ipv4.ip_forward_update_priority = 1
net.ipv4.ip_forward_use_pmtu = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.all.mc_forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.default.mc_forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth0.mc_forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth1.mc_forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv6.conf.lo.mc_forwarding = 0
[root@server services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server services]# sysctl -p /etc/sysctl.d/90-forward.conf
bash: sysctl: command not found...
Similar command is: 'sysctl'
[root@server services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server services]# firewall-cmd --zone=public --add-masquerade --permanent
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page
firewall-cmd: error: unrecognized arguments: --add-masquerade
[root@server services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server services]# firewall-cmd --reload
success
[root@server services]#
```

Рис. 2.6: Включение перенаправления пакетов и включение маскардинга

2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

На VM 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. 2.7).



```
[root@server services]# cd /vagrant/provision/server
[root@server server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/services/
[root@server server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d/
[root@server server]# cd /vagrant/provision/server
[root@server server]# touch firewall.sh
[root@server server]# chmod +x firewall.sh
[root@server server]#
```

Рис. 2.7: Создание каталогов и копирование конфигурационных файлов, создание скрипта firewall.sh

Редактирую скрипт (рис. 2.8).



Рис. 2.8: 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/.

2. 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"/>
```

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 маскарadingом (masquerading)?

- Разница между трансляцией сетевых адресов (NAT) и маскарadingом (masquerading) заключается в том, что в случае NAT исходный IP-адрес пакета заменяется на IP-адрес маршрутизатора, а в случае маскарadingа используется маршрутизатора.

5. 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
```

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

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