

# **Лабораторная работа №7**

**Расширенные настройки межсетевого экрана**

Андреева Софья Владимировна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
3.1	Создание пользовательской службы firewalld . . . . .	6
3.2	Перенаправление портов . . . . .	8
3.3	Настройка Port Forwarding и Masquerading . . . . .	8
3.4	Внесение изменений в настройки внутреннего окружения виртуальной машины . . . . .	10
<b>4</b>	<b>Контрольные вопросы</b>	<b>12</b>
<b>5</b>	<b>Выводы</b>	<b>13</b>

## Список иллюстраций

3.1	Содержание файла службы ssh . . . . .	6
3.2	Редактирование файла службы SSh . . . . .	7
3.3	Список доступным FirewoIID служб . . . . .	7
3.4	Добавление новой службы и её активация . . . . .	7
3.5	Получение клиентом удаленного доступа по SSH к серверу через порт 2022 . . . . .	8
3.6	Настройка перенаправления IPv4-пакетов и включение маскардинга . . . . .	9
3.7	Доступность выхода в Интернет на клиенте. . . . .	9
3.8	Создание окружения для внесения изменений в настройки окружающей среды . . . . .	10
3.9	Содержание firewall.sh . . . . .	10
3.10	Изменение файла Vagrantfile . . . . .	11

# 1 Цель работы

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

## 2 Задание

1. Настройте межсетевой экран виртуальной машины `server` для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022.
2. Настройте Port Forwarding на виртуальной машине `server`.
3. Настройте маскердинг на виртуальной машине `server` для организации доступа клиента к сети Интернет.
4. Напишите скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внести изменения в Vagrantfile

## 3 Выполнение лабораторной работы

### 3.1 Создание пользовательской службы firewalld

Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом. Затем запустим виртуальную машину server

На основе существующего файла описания службы ssh создадим файл с собственным описанием, посмотрим его содержимое(рис. fig. 3.1):

```
[root@server svandeeva: ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server svandeeva: ~]# 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 commands on remote machines. It provides secure encrypted communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the openssh-server package installed for this option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server svandeeva: ~]#
```

Рис. 3.1: Содержание файла службы ssh

В первой строчке этого файла указана версия xml и используемая кодировка - utf8. Затем указаны тег service, а внутри его тег-потомок short, внутри которого указано SSH. Также внутри указан тег description, внутри которого написано описание протокола ssh, и указан протокол передачи порта tcp и н номер порта 22.

Откроем файл описания службы на редактирование и заменим порт 22 на новый порт (2022) и скорректируем описание службы(рис. fig. 3.2):

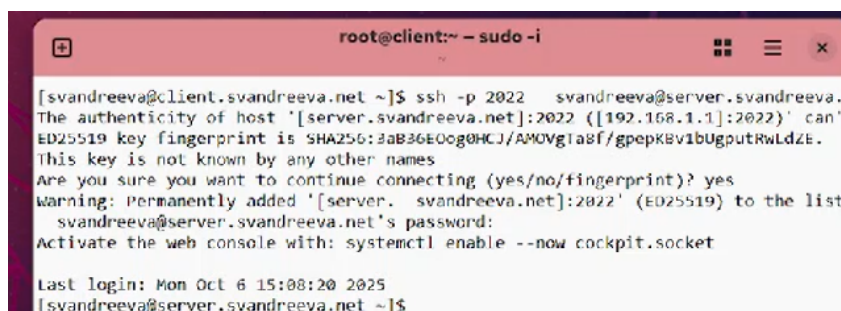


## 3.2 Перенаправление портов

Организуем на сервере переадресацию с порта 2022 на порт 22 с помощью команды:

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

На клиенте попробуем получить доступ по SSH к серверу через порт 2022(рис. fig. 3.5):



```
root@client:~ - sudo -i
[svandreeva@client.svandreeva.net ~]$ ssh -p 2022 svandreeva@server.svandreeva.
The authenticity of host '[server.svandreeva.net]:2022 ([192.168.1.1]:2022)' can'
E025519 key fingerprint is SHA256:3aB36E0og0HCJ/AMOVgIa8f/gpepKv1bUgputrWldzE.
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.svandreeva.net]:2022' (E025519) to the list
svandreeva@server.svandreeva.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Oct 6 15:08:20 2025
[svandreeva@server.svandreeva.net ~]$
```

Рис. 3.5: Получение клиентом удаленного доступа по SSH к серверу через порт 2022

## 3.3 Настройка Port Forwarding и Masquerading

На сервере посмотрим, активирована ли в ядре системы возможность перенаправления IPv4-пакетов, затем включим пренаправление IPv4-пакетов на сервере и включим маскарадинг на сервере(fig. 3.6):



```
[root@server.svandreeva.net ~]# sysctl -a | grep forward
net.ipv4.conf.all.bc_forwarding = 0
net.ipv4.conf.all.forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.default.bc_forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.eth0.bc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth1.bc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.lo.bc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
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.svandreeva.net ~]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.svandreeva.net ~]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.svandreeva.net ~]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.svandreeva.net ~]# firewall-cmd --reload
success
[root@server.svandreeva.net ~]#
```

Рис. 3.6: Настройка перенаправления IPv4-пакетов и включение маскардинга

Теперь проверим доступность выхода в Интернет на клиенте.

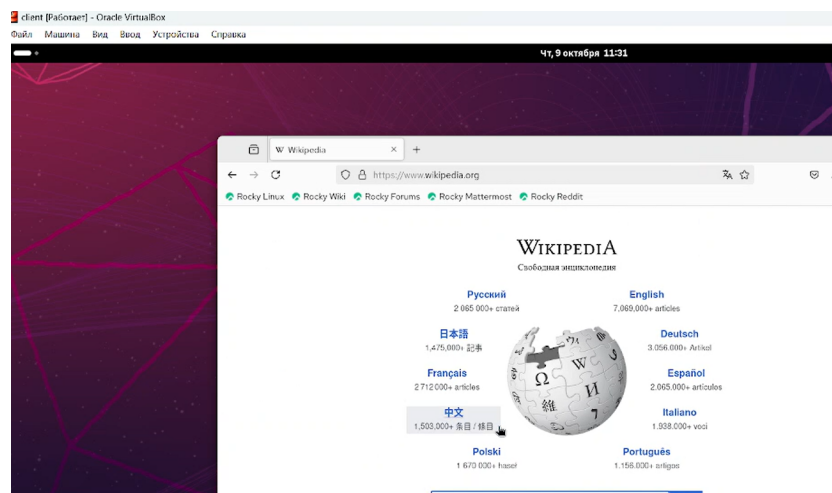


Рис. 3.7: Доступность выхода в Интернет на клиенте.

### 3.4 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 и создадим исполняемый файл `firewall.sh` (рис. fig. 3.8)

```
[root@server:svandreeva.net ~]# echo 'net.ipv4.ip_forward = 1' > /etc/sysctl.d/90-forward.conf
[root@server:svandreeva.net ~]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server:svandreeva.net ~]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server:svandreeva.net ~]# firewall-cmd --reload
success
[root@server:svandreeva.net ~]# cd /vagrant/provision/server
[root@server:svandreeva.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server:svandreeva.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server:svandreeva.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/services/
[root@server:svandreeva.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d/
[root@server:svandreeva.net server]# cd /vagrant/provision/server
[root@server:svandreeva.net server]# touch firewall.sh
[root@server:svandreeva.net server]# chmod +x firewall.sh
```

Рис. 3.8: Создание окружения для внесения изменений в настройки окружающей среды

Открыв `firewall.sh` на редактирование, пропишем в нём следующий скрипт (fig. 3.9):

```
root@server:/vagrant/provision/server - sudo -i
#!/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
```

Рис. 3.9: Содержание `firewall.sh`

Для отработки созданного скрипта во время загрузки виртуальной машины `server` в конфигурационном файле `Vagrantfile` добавим в разделе конфигурации для сервера (fig. 3.10):

```

C: > work > svandreeva > vagrant > Vagrantfile
 4  Vagrant.configure("2") do |config|
24    config.vm.define "server", autostart: false do |server|
33
34      server.vm.network :private_network,
35      |               | ip: "192.168.1.1",
36      |               | virtualbox__intnet: true
37
38      server.vm.provision "server dummy",
39      |               | type: "shell",
40      |               | preserve_order: true,
41      |               | path: "provision/server/01-dummy.sh"
42
43      server.vm.provision "server dns",
44      |               | type: "shell",
45      |               | preserve_order: true,
46      |               | path: "provision/server/dns.sh"
47
48      server.vm.provision "server dhcp",
49      |               | type: "shell",
50      |               | preserve_order: true,
51      |               | path: "provision/server/dhcp.sh"
52      server.vm.provision "server http",
53      |               | type: "shell",
54      |               | preserve_order: true,
55      |               | path: "provision/server/http.sh"
56
57      server.vm.provision "server mysql",
58      |               | type: "shell",
59      |               | preserve_order: true,
60      |               | path: "provision/server/mysql.sh"
61      server.vm.provision "server firewall",
62      |               | type: "shell",
63      |               | preserve_order: true,
64      |               | path: "provision/server/firewall.sh"
65

```

Рис. 3.10: Изменение файла Vagrantfile

## 4 Контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?

`/usr/lib/firewalld/services/s`

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 маскарadingом (masquerading)?

При маскарadingе вместо адреса отправителя(как делается это в NAT) динамически подставляется адрес назначенного интерфейса (сетевой адрес + порт).

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

`sudo firewall-cmd --add-forward-port=port=4404:proto=tcp:toport=22:toaddr=10.0.0.10`

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

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

## 5 Выводы

В результате выполнения данной работы были приобретены практические навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.