

## **Лабораторная работа № 7**

### **Расширенные настройки межсетевого экрана**

**Абд эль хай мохамад**

## Содержание

<b><i>Цель работы</i></b> .....	<b>2</b>
<b><i>Выполнение лабораторной работы</i></b> .....	<b>2</b>
Создание пользовательской службы firewalld.....	2
Перенаправление портов.....	4
Настройка Port Forwarding и Masquerading.....	5
Внесение изменений в настройки внутреннего окружения виртуальной машины .....	6
<b>Вывод</b> .....	<b>7</b>
<b>Ответы на контрольные вопросы</b> .....	<b>7</b>

## ***Цель работы***

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

## ***Выполнение лабораторной работы***

### Создание пользовательской службы firewalld

1. На основе существующего файла описания службы ssh создаю файл с собственным описанием:

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

2. Просматриваю содержимое файла службы:

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

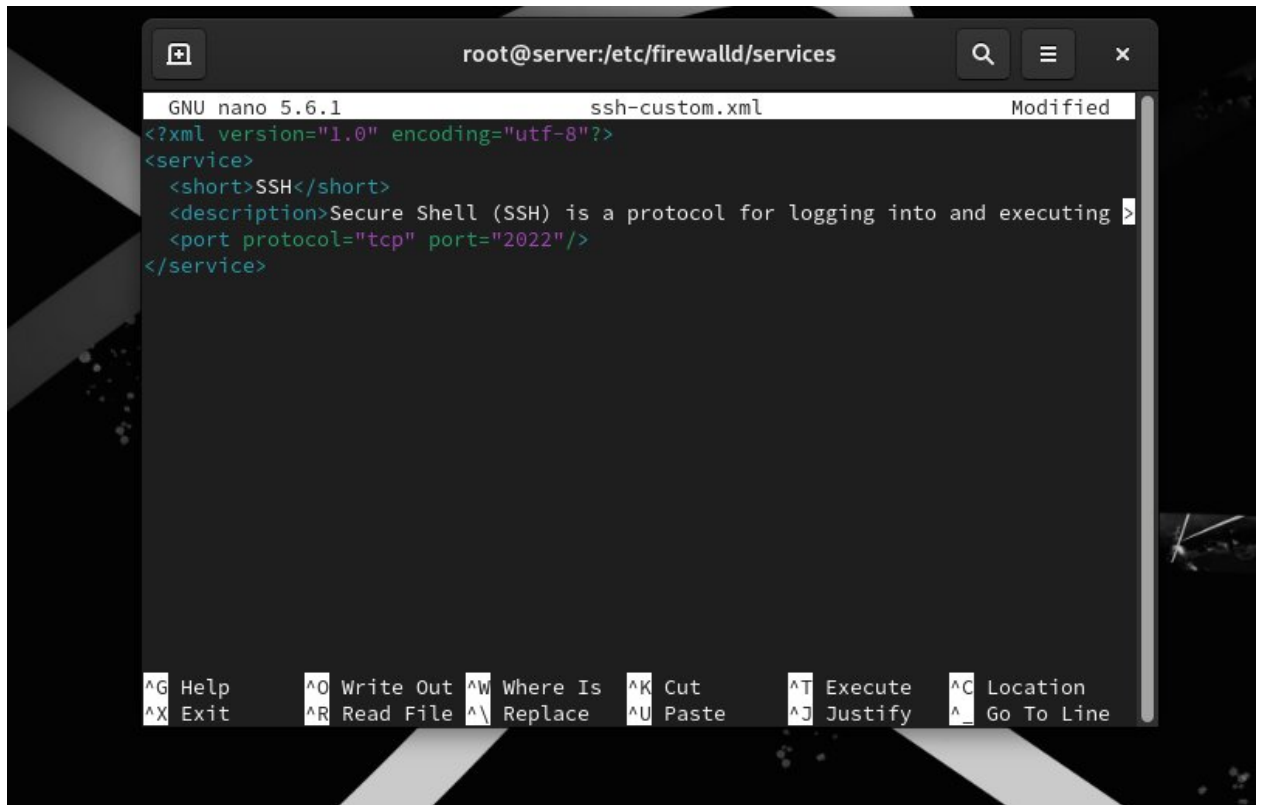
Первой строкой идёт объявление XML - указывает версию языка, на которой написан документ и метод кодировки документа.

Корневые элементы `<service>` и `</service>` - начало и конец описания сервиса.

Далее идут краткое и полное описание службы и настройка прослушивания порта 22.

3. Открываю файл описания службы на редактирование и заменяю порт 22 на новый порт (2022): `<port protocol="tcp" port="2022"/>`

Изменяю поля `<short>` и `<description>` добавляя описание для демонстрации, что это модифицированный файл службы.



4. Просматриваю список доступных FirewallD служб:

```
firewall-cmd --get-services
```

Новая служба ещё не отображается в списке.

5. 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
```

Созданная служба отображается в списке доступных для FirewallD служб, но не активирована.

6. Добавляю новую службу в FirewallD и вывожу на экран список активных служб:

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

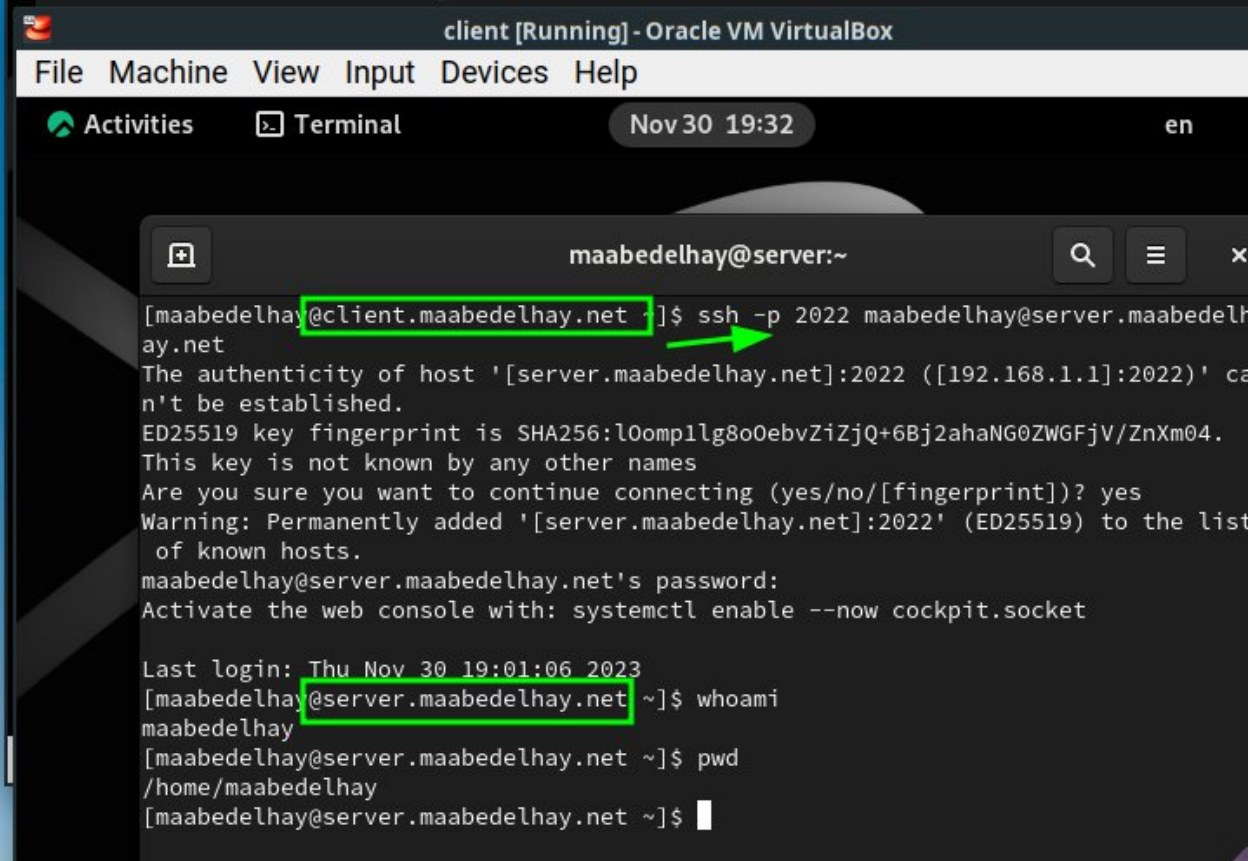
```
firewall-cmd --list-services
```

## Перенаправление портов

1. Организовываю на сервере переадресацию с порта 2022 на порт 22:

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

2. На клиенте получаю доступ по SSH к серверу через порт 2022:



The screenshot shows a terminal window titled "client [Running] - Oracle VM VirtualBox". The terminal output shows an SSH connection from a client to a server. The client's prompt is [maabeldelhay@client.maabeldelhay.net ~]. The command executed is ssh -p 2022 maabeldelhay@server.maabeldelhay.net. The server's prompt is maabeldelhay@server:~. The terminal output shows the SSH connection process, including the warning about the host's authenticity and the successful connection. The client's prompt is [maabeldelhay@client.maabeldelhay.net ~]. The server's prompt is maabeldelhay@server:~. The terminal output shows the command whoami being executed, which returns maabeldelhay. The terminal output shows the command pwd being executed, which returns /home/maabeldelhay. The terminal output shows the command being executed, which returns [maabeldelhay@server.maabeldelhay.net ~].

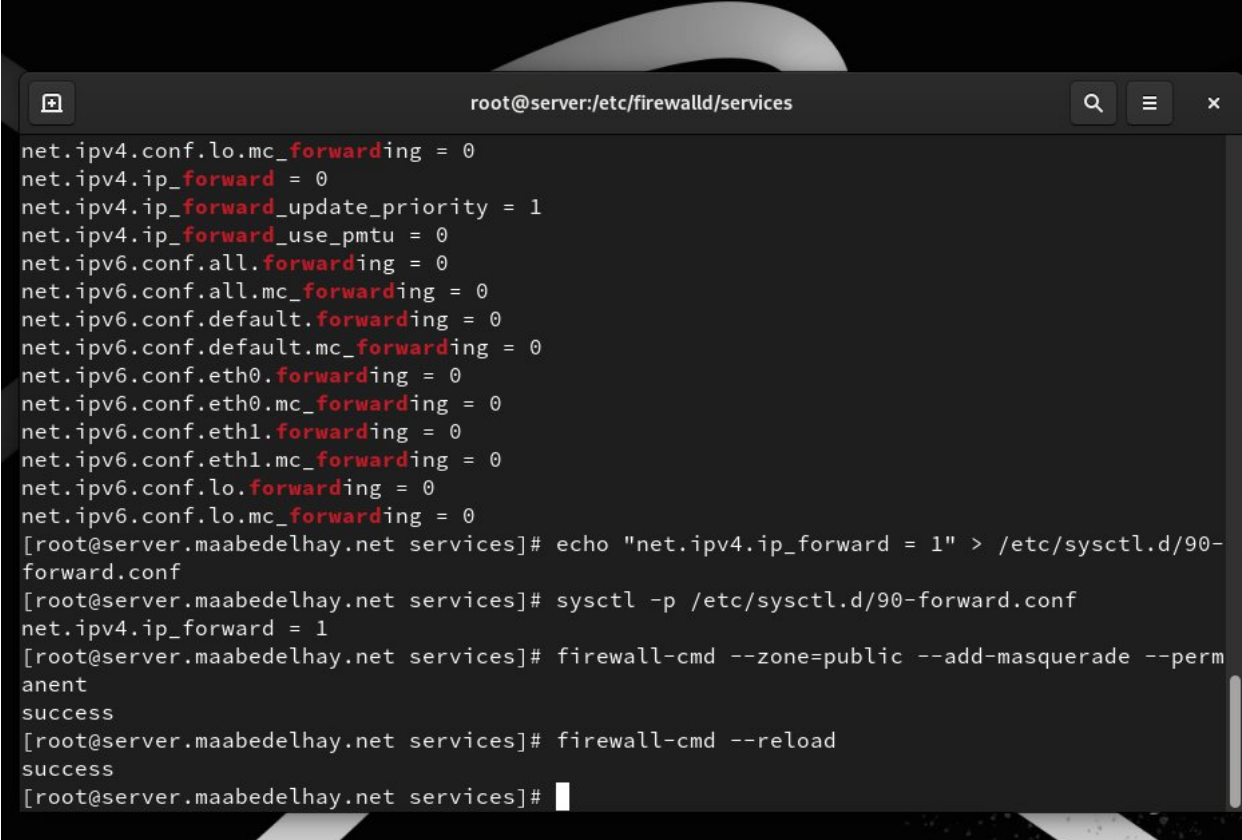
```
client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Nov 30 19:32 en
maabeldelhay@server:~
[maabeldelhay@client.maabeldelhay.net ~]$ ssh -p 2022 maabeldelhay@server.maabeldelhay.net
The authenticity of host '[server.maabeldelhay.net]:2022 ([192.168.1.1]:2022)' can't be established.
ED25519 key fingerprint is SHA256:l0omp1lg8o0ebvZiZjQ+6Bj2ahaNG0ZWGFjV/ZnXm04.
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.maabeldelhay.net]:2022' (ED25519) to the list of known hosts.
maabeldelhay@server.maabeldelhay.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Thu Nov 30 19:01:06 2023
[maabeldelhay@server.maabeldelhay.net ~]$ whoami
maabeldelhay
[maabeldelhay@server.maabeldelhay.net ~]$ pwd
/home/maabeldelhay
[maabeldelhay@server.maabeldelhay.net ~]$
```

## Настройка Port Forwarding и Masquerading

1. На сервере просматриваю, активирована ли в ядре системы возможность перенаправления IPv4-пакетов:

```
sysctl -a | grep forward
```

A screenshot of a terminal window titled 'root@server:/etc/firewalld/services'. The terminal shows the output of 'sysctl -a | grep forward', listing various network forwarding settings for IPv4 and IPv6, all set to 0. Subsequent commands include creating a file '/etc/sysctl.d/90-forward.conf' with 'net.ipv4.ip\_forward = 1', applying it with 'sysctl -p', adding a masquerade rule for the public zone with 'firewall-cmd --zone=public --add-masquerade --permanent', and finally reloading the firewall with 'firewall-cmd --reload'.

```
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.maabeldelhay.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.maabeldelhay.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.maabeldelhay.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.maabeldelhay.net services]# firewall-cmd --reload
success
[root@server.maabeldelhay.net services]#
```

2. Включаю 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
```
3. Включаю маскардинг на сервере:  

```
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload
```
4. На клиенте проверяю доступность выхода в Интернет.

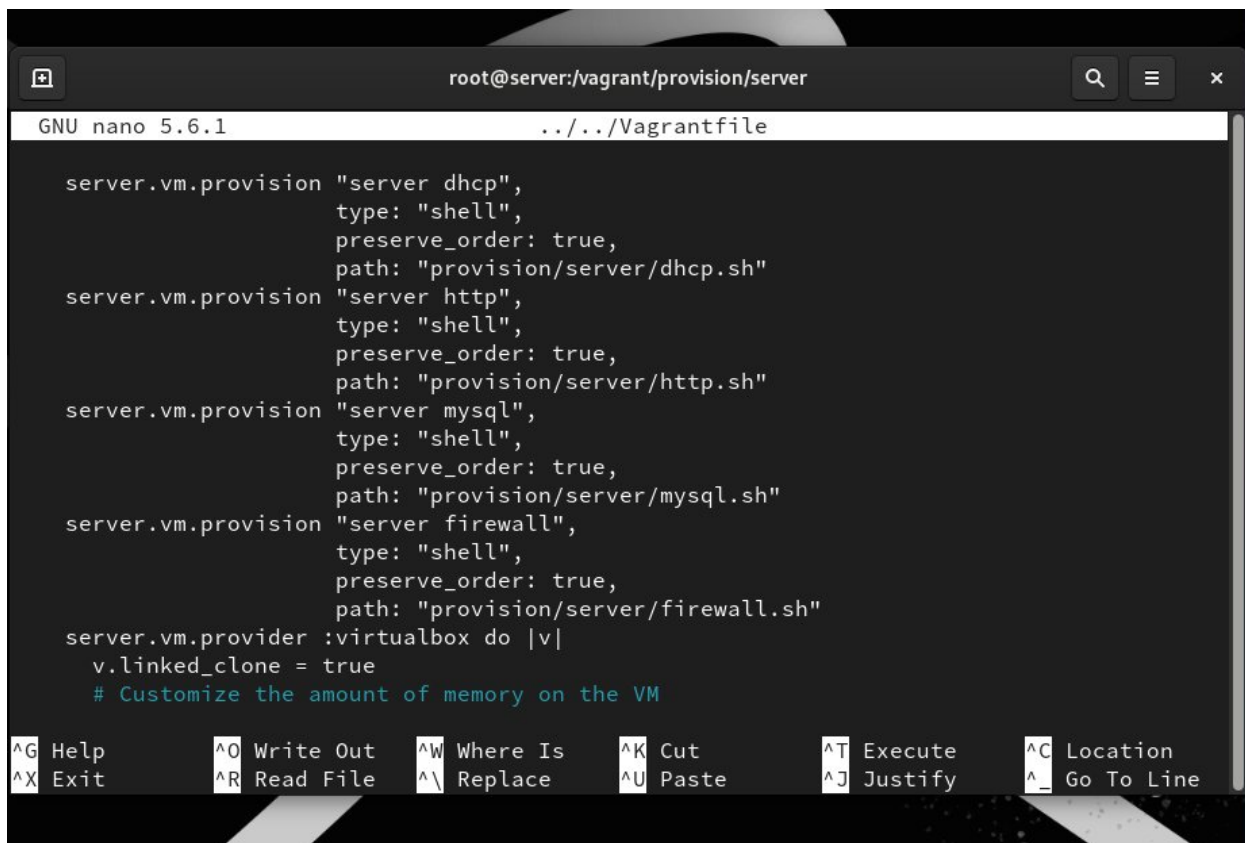
## Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перехожу в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создаю в нём каталог `firewall`, в который помещаю в соответствующие подкаталоги конфигурационные файлы FirewallD:

```
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/
```

2. В каталоге `/vagrant/provision/server` создаю файл `firewall.sh`:

```
cd /vagrant/provision/server
touch firewall.sh
chmod +x firewall.sh
Открыв его на редактирование, прописываю в нём следующий скрипт:
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/firewall/etc/* /etc
echo "Configure masquerading"
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload
restorecon -vR /etc
```



The screenshot shows a terminal window with the title bar 'root@server:/vagrant/provision/server'. The editor is GNU nano 5.6.1, editing the file ../../Vagrantfile. The content of the file is as follows:

```
server.vm.provision "server dhcp",
  type: "shell",
  preserve_order: true,
  path: "provision/server/dhcp.sh"
server.vm.provision "server http",
  type: "shell",
  preserve_order: true,
  path: "provision/server/http.sh"
server.vm.provision "server mysql",
  type: "shell",
  preserve_order: true,
  path: "provision/server/mysql.sh"
server.vm.provision "server firewall",
  type: "shell",
  preserve_order: true,
  path: "provision/server/firewall.sh"
server.vm.provider :virtualbox do |v|
  v.linked_clone = true
  # Customize the amount of memory on the VM
```

The bottom of the window shows a status bar with various keyboard shortcuts: ^G Help, ^X Exit, ^O Write Out, ^R Read File, ^W Where Is, ^\ Replace, ^K Cut, ^U Paste, ^T Execute, ^J Justify, ^C Location, ^\_ Go To Line.

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

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

## Вывод

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

## Ответы на контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?  
/etc/firewalld
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)?  
В случае NAT адрес указывается явно (это предполагает, что он известен на этапе создания правила, а для динамического адреса это не всегда так), а в случае маскарadingа - адрес автоматически берётся с интерфейса.  
Ещё одной особенностью маскарadingа (в iptables) является «забывание» про установленные трансляции при остановке (down) интерфейса. Это связано с тем, что после поднятия интерфейса его адрес, вероятнее всего (в случае DHCP/Dialup) будет другим, и записи о ранее выполненных трансляциях не будут иметь смысла.
  
5. 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=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