

# **Отчёт по лабораторной работе №7**

**Администрирование сетевых подсистем**

Ищенко Ирина НПИбд-02-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>13</b>
<b>4</b>	<b>Ответы на контрольные вопросы</b>	<b>14</b>

## Список иллюстраций

2.1	Создание собственного файла описания службы и просмотр . . . .	6
2.2	Редактирование файла описания службы . . . . .	7
2.3	Список доступных служб . . . . .	7
2.4	Новая служба в списке доступных служб . . . . .	8
2.5	Добавление новой службы и просмотр списка активных служб, со- хранение информации о состоянии . . . . .	8
2.6	Переадресация . . . . .	9
2.7	Доступ по SSH к серверу через порт 2022 на клиенте . . . . .	9
2.8	Возможность перенаправления пакетов . . . . .	10
2.9	Включение перенаправления пакетов и включение маскардинга	10
2.10	Браузер клиента . . . . .	11
2.11	Внесение изменений в настройки внутреннего окружения . . . . .	11
2.12	Создание скрипта firewall.sh . . . . .	12
2.13	Vagrantfile . . . . .	12

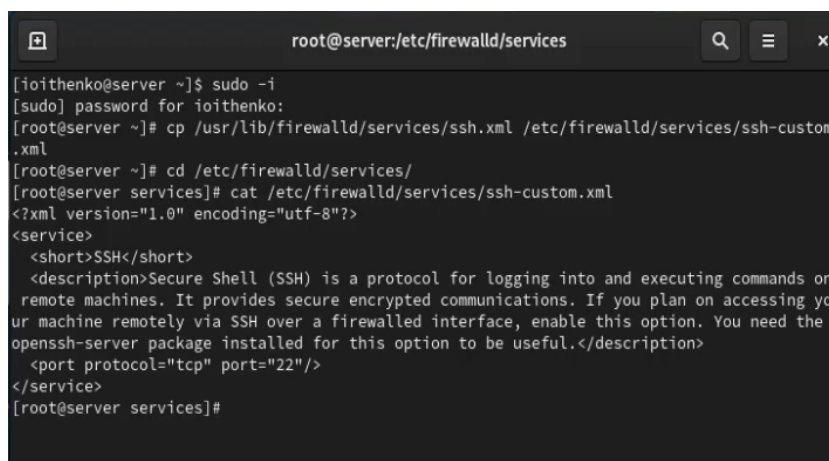
## **Список таблиц**

# 1 Цель работы

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

## 2 Выполнение лабораторной работы

Запускаем ВМ через рабочий каталог. На ВМ server входим под собственным пользователем и переходим в режим суперпользователя. На основе существующего файла описания службы ssh создаем файл с собственным описанием. Просматриваем содержимое файла (рис. 2.1).

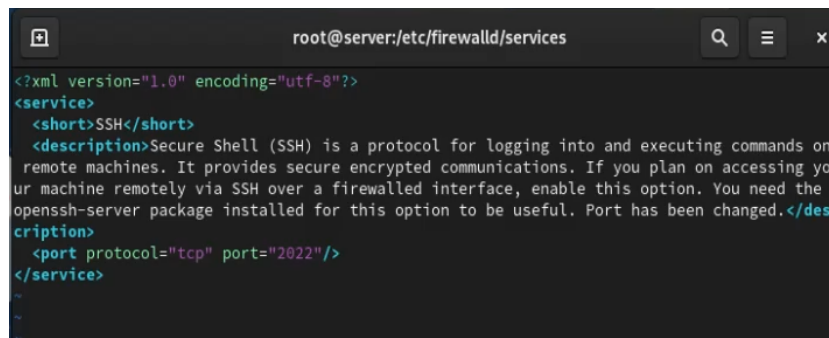


```
root@server:/etc/firewalld/services

[ioithenko@server ~]$ sudo -i
[sudo] password for ioithenko:
[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 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 services]#
```

Рис. 2.1: Создание собственного файла описания службы и просмотр

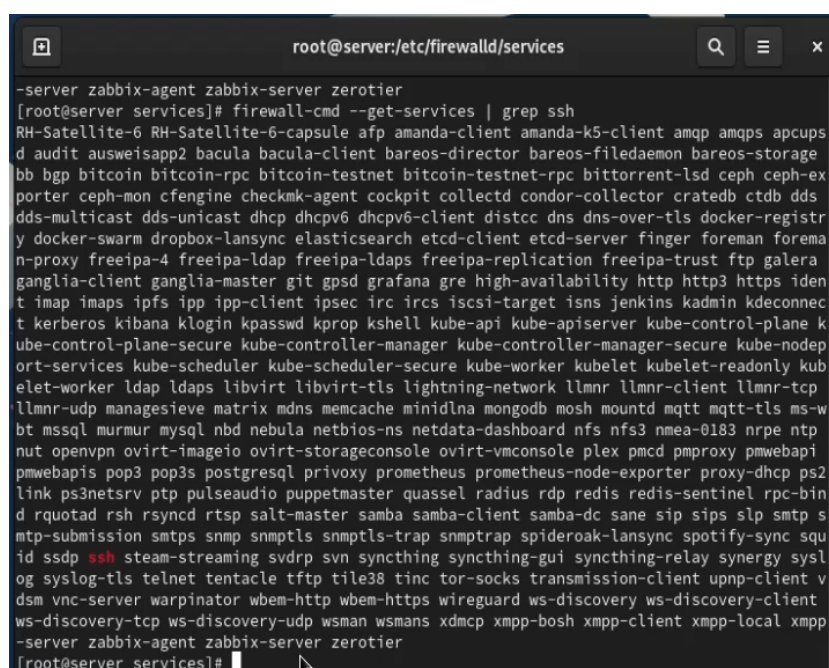
Открываем файл на редактирование и меняем порт 22 на порт 2022, в описании службы указав, что порт был изменен (рис. 2.2)



```
root@server:/etc/firewalld/services
<?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 yo
ur machine remotely via SSH over a firewalled interface, enable this option. You need the
openssh-server package installed for this option to be useful. Port has been changed.</des
cription>
  <port protocol="tcp" port="2022"/>
</service>
```

Рис. 2.2: Редактирование файла описания службы

Просматриваем список доступных служб (новой службы пока нет) (рис. 2.3).



```
root@server:/etc/firewalld/services
-server zabbix-agent zabbix-server zerotier
[root@server services]# firewall-cmd --get-services | grep ssh
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcups
d audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage
bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-ex
porter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctddb dds
dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registr
y docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman forema
n-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera
ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https iden
t imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnec
t kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane k
ube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodet
ort-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kub
elet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp
llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-w
bt mssql murmur mysql nbd nebula netbios-ns netdata-dashboad nfs nfs3 nmea-0183 nrpe ntp
nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi
pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2
link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bin
d rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips sip smtp s
mtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squ
id sddp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy sysl
og syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client v
dsm vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client
ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp
-server zabbix-agent zabbix-server zerotier
[root@server services]#
```

Рис. 2.3: Список доступных служб

Перезагружаем правила межсетевого экрана, снова просматриваем список доступных служб и видим новую (рис. 2.4).

```
root@server:/etc/firewalld/services
success
[root@server services]# firewall-cmd --get-services | grep ssh
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcups
d audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage
bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-ex
porter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds
dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registr
y docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman forema
n-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera
ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https iden
t imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnec
t kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane k
ube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodep
ort-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kub
elet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp
llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-w
bt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp
nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi
pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2
link ps3netdrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bin
d rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp s
mtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squ
id ssdp ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay s
ynergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client up
np-client vdsim vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discov
ery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp
-local xmpp-server zabbix-agent zabbix-server zerotier
[root@server services]#
```

Рис. 2.4: Новая служба в списке доступных служб

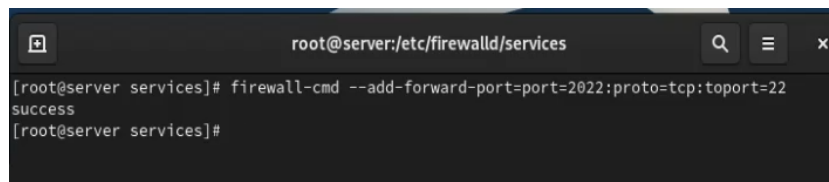
Новая служба отображается в списке доступных, но пока не активирована. Добавляем новую службу в FirewallD и просматриваем список активных служб (служба появилась). Перегружаем правила межсетевого экрана с сохранением информации о состоянии (рис. 2.5)

```
[root@server services]# firewall-cmd --list-services | grep ssh
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 | grep ssh
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. 2.5: Добавление новой службы и просмотр списка активных служб, сохранение информации о состоянии

Организовываем переадресацию с порта 2022 на порт 22 на сервере(рис. 2.6).

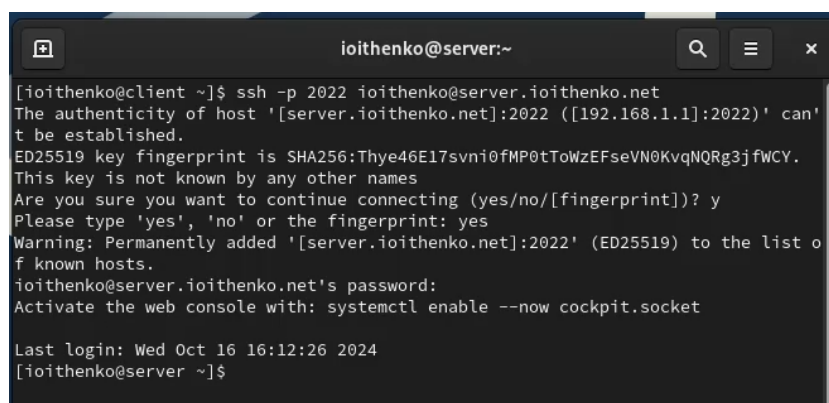


A terminal window titled 'root@server:/etc/firewalld/services'. The prompt is '[root@server services]#'. The command entered is 'firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22'. The output is 'success'. The prompt returns to '[root@server services]#'.

```
root@server:/etc/firewalld/services
[root@server services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
[root@server services]#
```

Рис. 2.6: Переадресация

На клиенте пробуем получить доступ по SSH через порт 2022. Доступ получен (рис. 2.7).

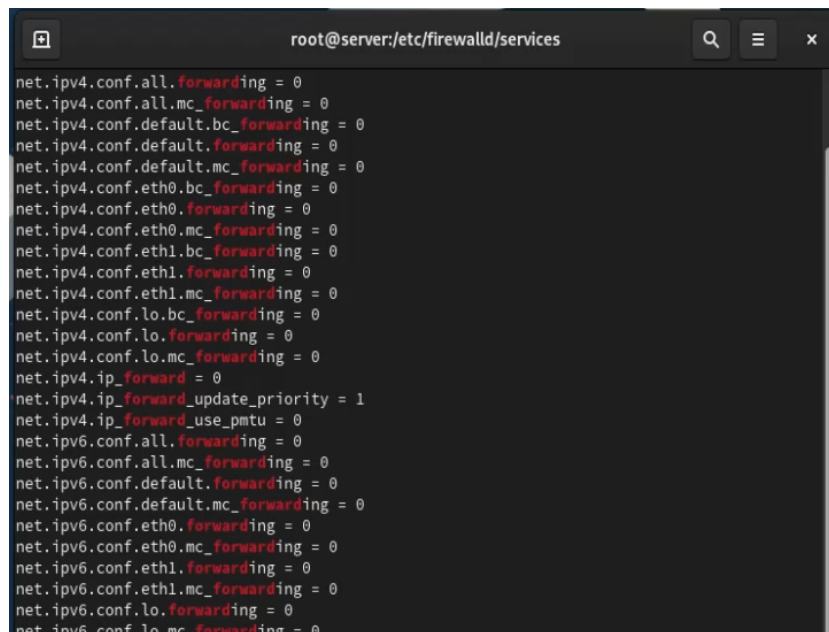
A terminal window titled 'ioithenko@server:~'. The prompt is '[ioithenko@client ~]\$'. The command entered is 'ssh -p 2022 ioithenko@server.ioithenko.net'. The output shows the SSH connection process, including host authenticity warnings and a successful login. The prompt returns to '[ioithenko@server ~]\$'.

```
ioithenko@server:~
[ioithenko@client ~]$ ssh -p 2022 ioithenko@server.ioithenko.net
The authenticity of host '[server.ioithenko.net]:2022 ([192.168.1.1]:2022)' can't
be established.
ED25519 key fingerprint is SHA256:Thye46E17svni0fMP0tToWzEFseVN0KvqNQRg3jfWCY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[server.ioithenko.net]:2022' (ED25519) to the list o
f known hosts.
ioithenko@server.ioithenko.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Oct 16 16:12:26 2024
[ioithenko@server ~]$
```

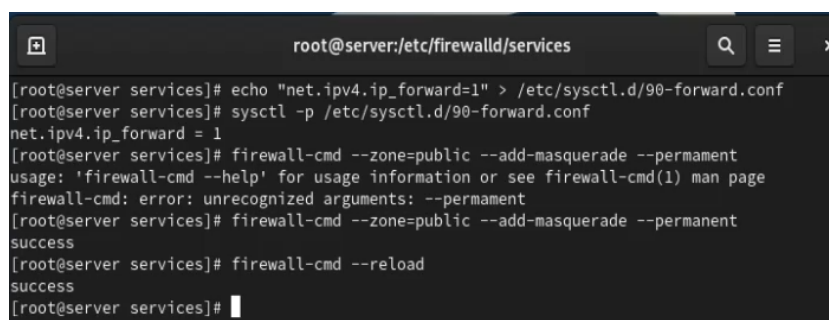
Рис. 2.7: Доступ по SSH к серверу через порт 2022 на клиенте

На сервере просматриваем, активирована ли в ядре системы возможность перенаправления IPv4-пакетов (рис. 2.8). Включаем перенаправление пакетов на сервере. Включаем маскарading на сервере (рис. 2.9). Убеждаемся, что на клиенте доступен выход в интернет (доступен) (рис. 2.10).



```
root@server:/etc/firewalld/services
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
```

Рис. 2.8: Возможность перенаправления пакетов



```
root@server:/etc/firewalld/services
[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
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: --permanent
[root@server services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server services]# firewall-cmd --reload
success
[root@server services]#
```

Рис. 2.9: Включение перенаправления пакетов и включение маскардинга

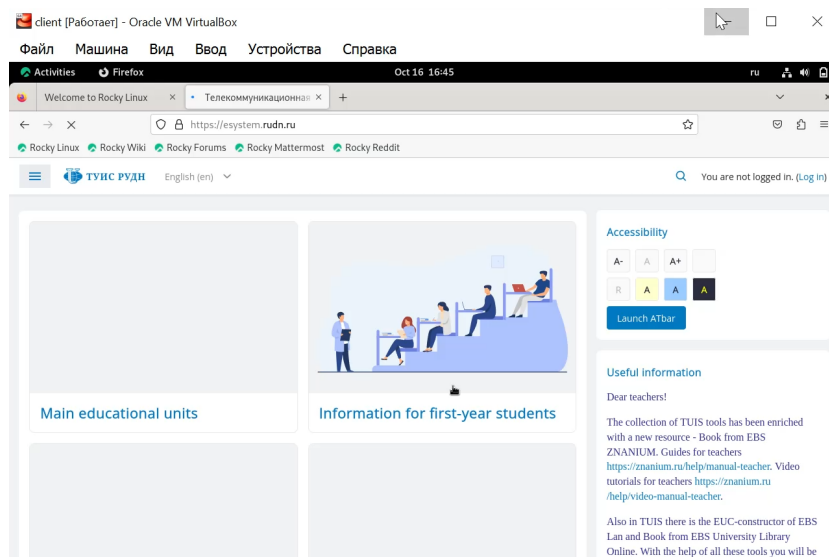


Рис. 2.10: Браузер клиента

На VM server перехожу в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/` и копирую в соответствующие каталоги конфигурационные файлы (рис. 2.11).

```

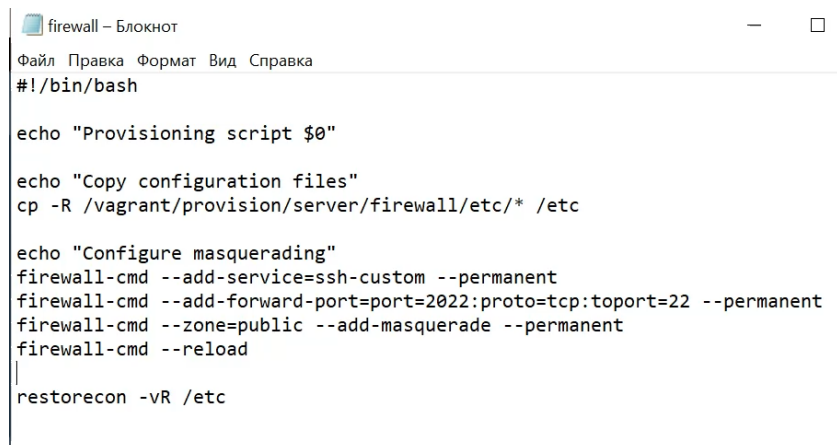
root@server:/vagrant/provision/server

[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]#

```

Рис. 2.11: Внесение изменений в настройки внутреннего окружения

Создаю скрипт `firewall.sh` (рис. 2.12).



```
firewall - Блокнот
Файл Правка Формат Вид Справка
#!/bin/bash

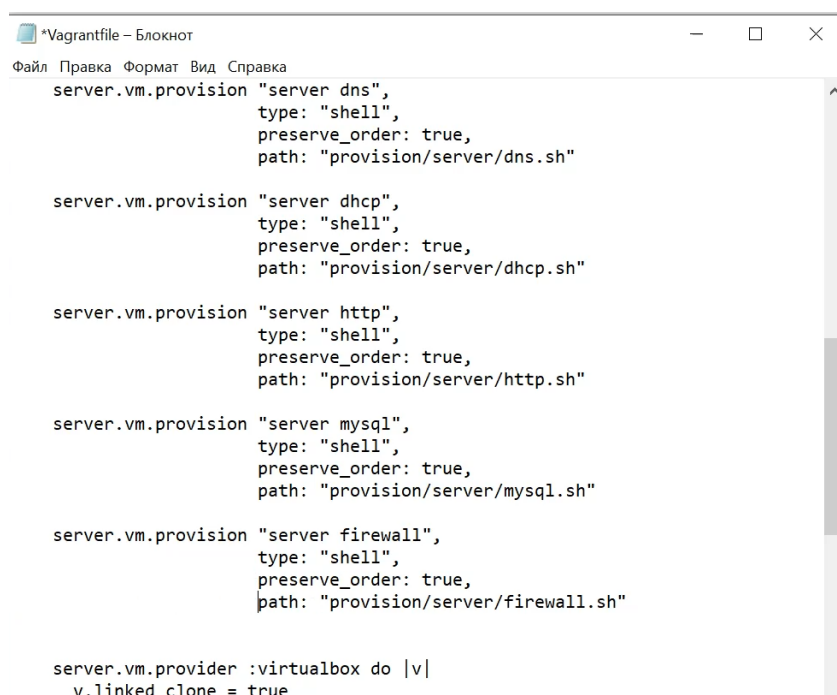
echo "Provisioning script $0"

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. 2.12: Создание скрипта firewall.sh

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавляем в разделе конфигурации для сервера следующую запись (рис. 2.13):



```
*Vagrantfile - Блокнот
Файл Правка Формат Вид Справка
server.vm.provision "server dns",
  type: "shell",
  preserve_order: true,
  path: "provision/server/dns.sh"

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
```

Рис. 2.13: Vagrantfile

## **3 Выводы**

В ходе лабораторной работы я получила 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