

# **Отчёт по лабораторной работе №7**

**Дисциплина: Администрирование сетевых подсистем**

Ибрахим Мохсейн Алькамаль

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение лабораторной работы</b>	<b>6</b>
2.1 Создание пользовательской службы firewalld . . . . .	6
2.2 Перенаправление портов . . . . .	8
2.3 Внесение изменений в настройки внутреннего . . . . .	11
<b>3 Выводы</b>	<b>13</b>
<b>4 Ответы на контрольные вопросы</b>	<b>14</b>

# Список иллюстраций

2.1	Копирование файла службы ssh.xml в ssh-custom.xml . . . . .	7
2.2	Редактирование службы: изменение порта на 2022 и обновление описания . . . . .	7
2.3	Добавление и активация пользовательской службы ssh-custom в firewalld . . . . .	8
2.4	Добавление и активация пользовательской службы ssh-custom в firewalld . . . . .	8
2.5	Настройка перенаправления порта 2022 на 22 в firewalld . . . . .	9
2.6	Подключение по SSH к серверу через порт 2022 с клиента . . . . .	9
2.7	Проверка параметров пересылки IPv4 в ядре системы . . . . .	10
2.8	Проверка доступа в Интернет с клиента после включения IP-forward и masquerade . . . . .	11
2.9	Создание структуры каталогов и копирование конфигурационных файлов FirewallD . . . . .	11
2.10	Содержимое provisioning-скрипта firewall.sh . . . . .	12
2.11	Добавление provisioning-скрипта firewall.sh в 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**

### **2.1 Создание пользовательской службы firewalld**

В рабочем каталоге проекта выполнен переход в режим суперпользователя на виртуальной машине `server`, после чего на основе существующего файла описания службы `ssh.xml` создан пользовательский файл `ssh-custom.xml` в каталоге `/etc/firewalld/services/` с помощью команды копирования. Далее осуществлён переход в соответствующий каталог для дальнейшей работы с файлом (рис. 2.1).

Содержимое файла `/etc/firewalld/services/ssh-custom.xml` выведено командой `cat`. Файл представляет собой XML-описание службы: корневой элемент `<service>`, краткое имя службы `<short>`, текстовое описание `<description>`, а также определение порта через элемент `<port>` с указанием протокола `tcp` и номера порта `22` (рис. 2.1).

```
[alkamal@server.alkamal.net ~]$ sudo -i
[sudo] password for alkamal:
[root@server.alkamal.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.alkamal.net ~]# cd /etc/firewalld/services/
[root@server.alkamal.net 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>
```

Рисунок 2.1: Копирование файла службы ssh.xml в ssh-custom.xml

Файл службы отредактирован: в элементе `<port>` изменён номер порта с 22 на 2022, а в элементе `<description>` указано, что используется модифицированная служба SSH для доступа через TCP-порт 2022. После редактирования содержимое файла повторно выведено на экран для проверки внесённых изменений (рис. 2.3).

```
[root@server.alkamal.net services]# nano /etc/firewalld/services/ssh-custom.xml
[root@server.alkamal.net services]# cat /etc/firewalld/services/ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Модифицированная служба SSH для доступа через порт TCP 2022 (лабораторная работа №7)</description>
  <port protocol="tcp" port="2022"/>
</service>
```

Рисунок 2.2: Редактирование службы: изменение порта на 2022 и обновление описания

С помощью команды `firewall-cmd --get-services` получен список доступных служб, затем выполнена перезагрузка правил межсетевого экрана командой `firewall-cmd --reload` (рис. 2.4). После перезагрузки служба `ssh-custom` отображается в списке доступных служб, но отсутствует среди активных . Далее служба добавлена в активные с помощью `firewall-cmd --add-service=ssh-custom`, проверена командой `firewall-cmd --list-services`, затем добавлена на постоянной основе с ключом `--permanent` и выполнена повторная перезагрузка правил (рис. 2.4).

```
[root@server.alkamal.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcup
sd audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage
e bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph
-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb
dds dds-multicast dds-unicast dhcp dhcpcv6 dhcpcv6-client distcc dns dns-over-tls docker-re
gistry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman
foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp
galera ganglia-client ganglia-master git gpgsql grafana gre high-availability http http3 ht
tps ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin
kdeconnect kerberos kibana klogind kpasswd kprop kshell kube-api kube-apiserver kube-contr
ol-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure
kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-
readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-clie
nt llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt
mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ms netdata-dashboard nfs nfs3 nmea
-n183 nntp ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsol
e plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus promethe
us-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius
rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-c
lient samba-dc sane sip sips slp smtp smtp-submission smtsp snmp snmpTLS snmpTLS-trap snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing s
yncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tinc t
or-socks transmission-client upnp-client vdsim 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.alkamal.net services]# firewall-cmd --reload
success
```

Рисунок 2.3: Добавление и активация пользовательской службы ssh-custom в firewalld

```
success
[root@server.alkamal.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcup
sd audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage
e bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph
-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb
dds dds-multicast dds-unicast dhcp dhcpcv6 dhcpcv6-client distcc dns dns-over-tls docker-re
gistry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman
foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp
galera ganglia-client ganglia-master git gpgsql grafana gre high-availability http http3 ht
tps ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin
kdeconnect kerberos kibana klogind kpasswd kprop kshell kube-api kube-apiserver kube-contr
ol-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure
kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-
readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-clie
nt llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt
mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ms netdata-dashboard nfs nfs3 nmea
-n183 nntp ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsol
e plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus promethe
us-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius
rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-c
lient samba-dc sane sip sips slp smtp smtp-submission smtsp snmp snmpTLS snmpTLS-trap snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn
syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp ti
le38 tinc tor-socks transmission-client upnp-client vdsim vnc-server warpinator wbem-http
wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp w
sman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
zerotier
[root@server.alkamal.net services]# firewall-cmd --list-services
cockpit dhcp dhcpcv6-client dns http https ssh
[root@server.alkamal.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.alkamal.net services]# firewall-cmd --list-services
cockpit dhcp dhcpcv6-client dns http https ssh ssh-custom
[root@server.alkamal.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.alkamal.net services]# firewall-cmd --reload
success
```

Рисунок 2.4: Добавление и активация пользовательской службы ssh-custom в firewalld

## 2.2 Перенаправление портов

На виртуальной машине `Server` выполнена настройка перенаправления трафика с TCP-порта 2022 на стандартный порт SSH 22 с помощью команды

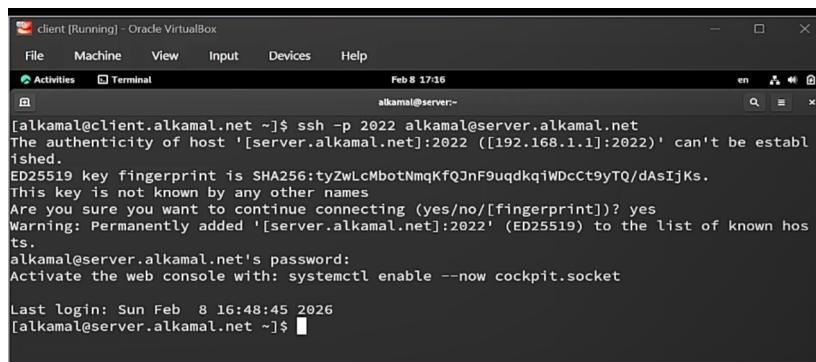
```
firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22.
```

Команда завершилась успешно, что подтверждает добавление правила переадресации в текущую конфигурацию firewalld (рис. 2.5).

```
[root@server.alkamal.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22  
success  
[root@server.alkamal.net services]#
```

Рисунок 2.5: Настройка перенаправления порта 2022 на 22 в firewalld

На виртуальной машине `client` выполнена попытка подключения к серверу по SSH через порт 2022 командой `ssh -p 2022 alkamal@server.alkamal.net`. При первом подключении подтверждена подлинность хоста и его ключ добавлен в файл `known_hosts`. После ввода пароля пользователя выполнен успешный вход в систему, что подтверждает корректную работу перенаправления с порта 2022 на порт 22 (рис. 2.6).



```
[alkamal@client.alkamal.net ~]$ ssh -p 2022 alkamal@server.alkamal.net  
The authenticity of host '[server.alkamal.net]:2022 ([192.168.1.1]:2022)' can't be established.  
ED25519 key fingerprint is SHA256:tyZwLcMbotNmqKfQJnF9uqdqkiWDccT9yTQ/dAsIjKs.  
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.alkamal.net]:2022' (ED25519) to the list of known hosts.  
alkamal@server.alkamal.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Sun Feb 8 16:48:45 2026  
[alkamal@server.alkamal.net ~]$
```

Рисунок 2.6: Подключение по SSH к серверу через порт 2022 с клиента

На виртуальной машине `server` выполнена проверка состояния параметров пересылки пакетов в ядре с помощью команды `sysctl -a | grep forward`. В выводе параметр `net.ipv4.ip_forward` имел значение 0, что означает отключённую маршрутизацию IPv4-пакетов (рис. 2.7).

Для включения пересылки IPv4-пакетов создан файл `/etc/sysctl.d/90-forward.conf` с параметром `net.ipv4.ip_forward = 1`, после чего конфигурация применена командой `sysctl -p /etc/sysctl.d/90-forward.conf`,

что подтвердило установку значения 1. Далее в зоне public активирован маскарадинг с помощью `firewall-cmd --zone=public --add-masquerade --permanent` и выполнена перезагрузка правил `firewall-cmd --reload` (рис. 2.7).

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

Рисунок 2.7: Проверка параметров пересылки IPv4 в ядре системы

На виртуальной машине client проверена доступность сети Интернет командами `ping 8.8.8.8` и `ping google.com`; получены ответы без потерь пакетов, что подтверждает корректную работу перенаправления и маскарадинга (рис. 2.8).

```
[client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 8 17:19
alkamal@server:~ x alkamal@client:~ x alkamal@client:~ x
[alkamal@client.alkamal.net ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=254 time=2.19 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=254 time=1.27 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=254 time=0.947 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=254 time=1.30 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=254 time=0.506 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=254 time=1.44 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=254 time=0.578 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6036ms
rtt min/avg/max/mdev = 0.506/1.175/2.190/0.531 ms
[alkamal@client.alkamal.net ~]$ ping google.com
PING google.com (64.233.162.138) 56(84) bytes of data.
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=1 ttl=254 time=2.57 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=2 ttl=254 time=1.37 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=3 ttl=254 time=0.877 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=4 ttl=254 time=1.11 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=5 ttl=254 time=0.821 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=6 ttl=254 time=2.54 ms
^X64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=7 ttl=254 time=0.333 ms
64 bytes from li-in-f138.1e100.net (64.233.162.138): icmp_seq=8 ttl=254 time=0.839 ms
^C
--- google.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7277ms
rtt min/avg/max/mdev = 0.333/1.308/2.574/0.771 ms
[alkamal@client.alkamal.net ~]$
```

Рисунок 2.8: Проверка доступа в Интернет с клиента после включения IP-forward и masquerade

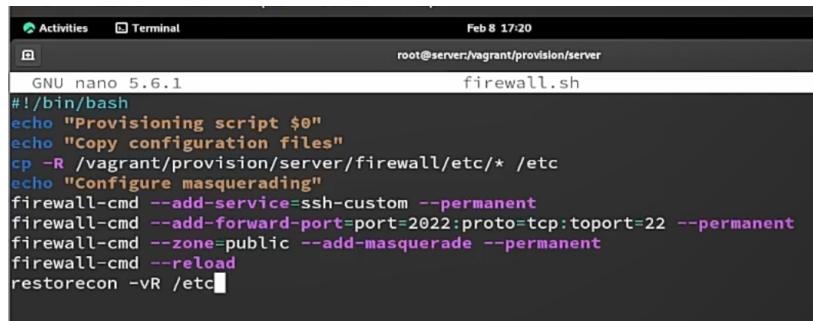
## 2.3 Внесение изменений в настройки внутреннего

На виртуальной машине server выполнен переход в каталог /vagrant/provision/server, после чего создана структура каталогов firewall/etc/firewalld/services и firewall/etc/sysctl.d. В данные каталоги скопированы файл пользовательской службы ssh-custom.xml и файл конфигурации 90-forward.conf, что обеспечивает сохранение настроек firewalld и параметра ip\_forward во внутреннем окружении виртуальной машины (рис. 2.9).

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

Рисунок 2.9: Создание структуры каталогов и копирование конфигурационных файлов FirewallD

В каталоге `/vagrant/provision/server` создан исполняемый файл `firewall.sh`, которому назначены права на выполнение. В скрипте реализовано копирование подготовленных конфигурационных файлов в каталог `/etc`, добавление службы `ssh-custom`, настройка перенаправления порта 2022 на 22, включение маскарадинга в зоне `public`, перезагрузка правил `firewalld` и восстановление контекстов SELinux командой `restorecon -vr /etc` (рис. 2.10).



```
GNU nano 5.6.1          Feb 8 17:20
root@server:/vagrant/provision/server
firewall.sh

#!/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
```

Рисунок 2.10: Содержимое provisioning-скрипта `firewall.sh`

В конфигурационный файл `Vagrantfile` в разделе настройки виртуальной машины `server` добавлен блок `provision` с типом `shell`, параметром `preserve_order: true` и указанием пути `provision/server/firewall.sh`. Это обеспечивает автоматическое выполнение созданного скрипта при запуске или пересоздании виртуальной машины (рис. 2.11).



```
C: > work > alkamal > vagrant > Vagrantfile
50   server.vm.provision "server firewall",
51     type: "shell",
52     preserve_order: true,
53     path: "provision/server/firewall.sh"
```

Рисунок 2.11: Добавление provisioning-скрипта `firewall.sh` в `Vagrantfile`

## **3 Выводы**

В ходе работы была создана пользовательская служба `ssh-custom` в системе `firewalld` с изменённым портом TCP 2022, что позволило организовать доступ к SSH через нестандартный порт. Реализовано перенаправление трафика с порта 2022 на порт 22, подтверждённое успешным подключением по SSH.

В ядре системы включена пересылка IPv4-пакетов (`net.ipv4.ip_forward = 1`), а также настроен маскарадинг в зоне `public`, что обеспечило корректную маршрутизацию и выход клиента в Интернет через сервер.

Конфигурационные файлы и параметры были вынесены во внутреннее окружение виртуальной машины и автоматизированы с помощью `provisioning`-скрипта `firewall.sh`, подключённого в `Vagrantfile`. Это обеспечивает воспроизводимость настроек при повторном развертывании виртуальной машины.

## 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:
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 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 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 маскарадинга IP- пакетов для всех пакетов, выходящих в зону public?

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