Лабораторная работа №7

Тема «Расширенные настройки межсетевого экрана»

по дисциплине «Администрирование сетевых подсистем»

Выполнил: Щербак Маргарита Романовна

Студент группы: НПИбд-02-21

«27» ноября 2023г.

Цель работы:

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

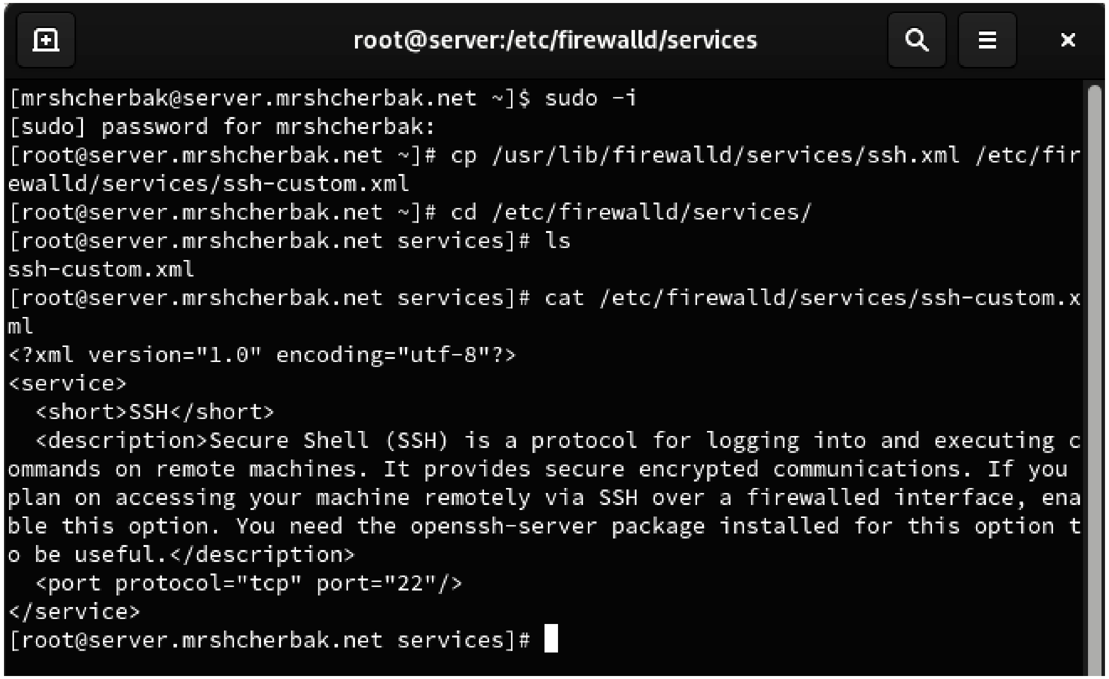
Задание

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

Выполнение работы

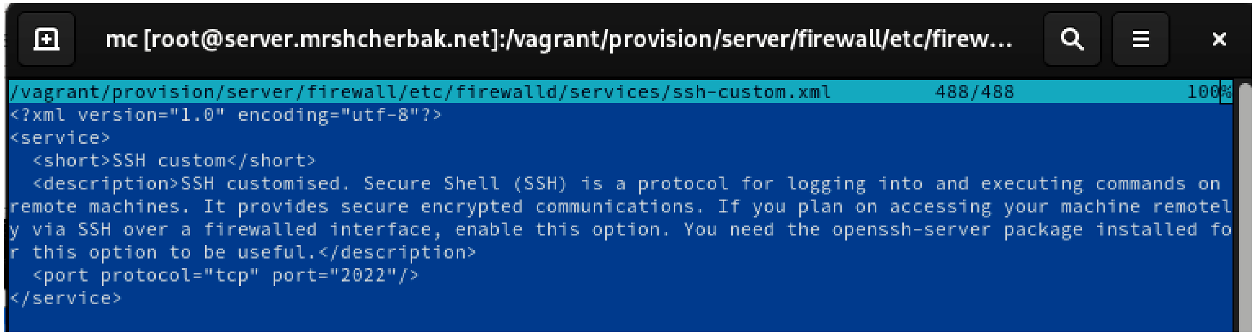
Создание пользовательской службы firewalld

Создание файла ssh-custom.xml и просмотр его содержимого

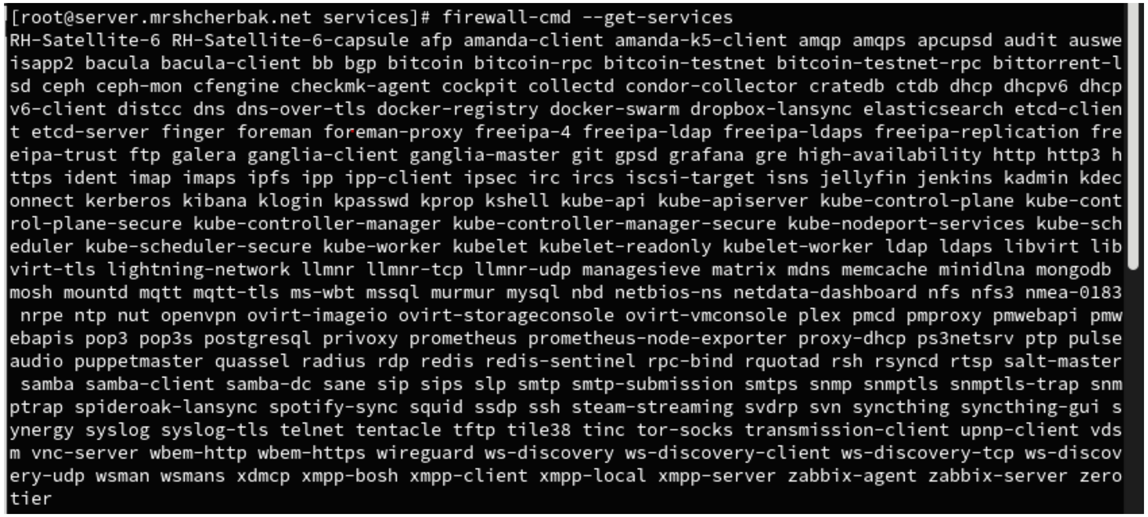


```
[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i
[sudo] password for mrshcherbak:
[root@server.mrshcherbak.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/fir
ewalld/services/ssh-custom.xml
[root@server.mrshcherbak.net ~]# cd /etc/firewalld/services/
[root@server.mrshcherbak.net services]# ls
ssh-custom.xml
[root@server.mrshcherbak.net services]# cat /etc/firewalld/services/ssh-custom.x
ml
<?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.mrshcherbak.net services]# 
```

Редактирование файла ssh-custom.xml

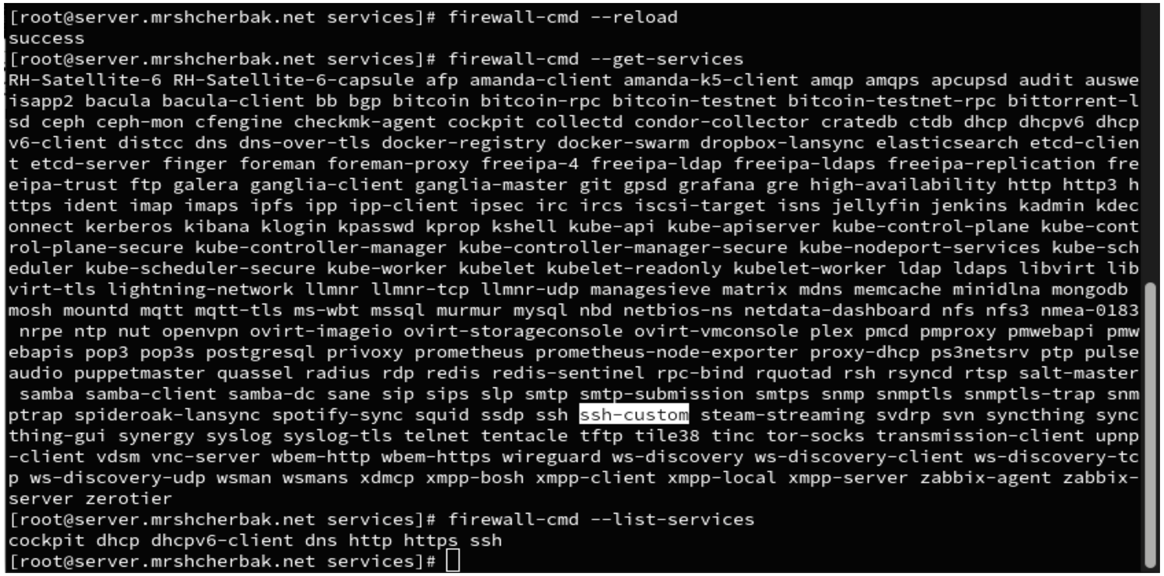

mc [root@server.mrshcherbak.net]:/vagrant/provision/server/firewall/etc/firew...

```
/vagrant/provision/server/firewall/etc/firewalld/services/ssh-custom.xml          488/488              100%
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH custom</short>
  <description>SSH customised. 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 remotel
y via SSH over a firewalled interface, enable this option. You need the openssh-server package installed fo
r this option to be useful.</description>
  <port protocol="tcp" port="2022"/>
</service>
```

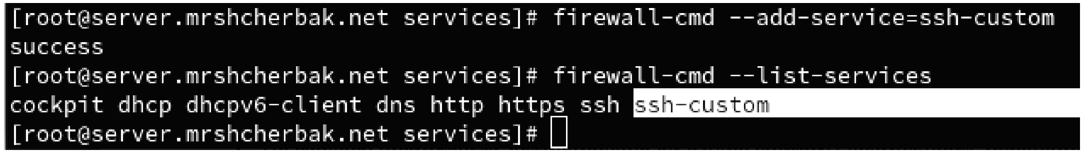


```
[root@server.mrshcherbak.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit auswe
isapp2 bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-l
sd ceph ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dhcp dhcpv6 dhcp
v6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-clien
t etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication fre
eipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 h
ttps ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jellyfin jenkins kadmin kdec
onnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-cont
rol-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-sch
eduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt lib
virt-tls lightning-network llmnr llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb
mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-dashboard nfs nfs3 nmea-0183
 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmw
ebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps3netsrv ptp pulse
audio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master
 samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui s
ynergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vds
m vnc-server wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discov
ery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zero
tier
```

Просмотр списка доступных FirewallD служб



```
[root@server.mrshcherbak.net services]# firewall-cmd --reload
success
[root@server.mrshcherbak.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit auswe
isapp2 bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-l
sd ceph ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dhcp dhcpv6 dhcp
v6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-clien
t etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication fre
eipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 h
ttps ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jellyfin jenkins kadmin kdec
onnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-cont
rol-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-sch
eduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt lib
virt-tls lightning-network llmnr llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb
mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-dashboard nfs nfs3 nmea-0183
 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmw
ebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps3netsrv ptp pulse
audio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master
 samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn syncthing sync
thing-gui synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp
-client vdsm vnc-server wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tc
p ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-
server zerotier
[root@server.mrshcherbak.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.mrshcherbak.net services]# 
```

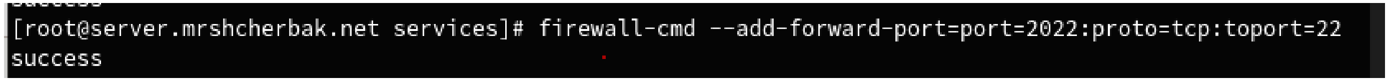


```
[root@server.mrshcherbak.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.mrshcherbak.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.mrshcherbak.net services]# 
```

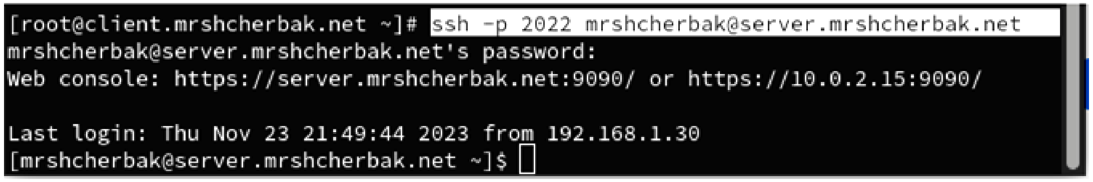
Служба активирована

Перенаправление портов

Организовала на сервере переадресацию с порта 2022 на порт 22. На клиенте попробовала получить доступ по SSH к серверу через порт 2022

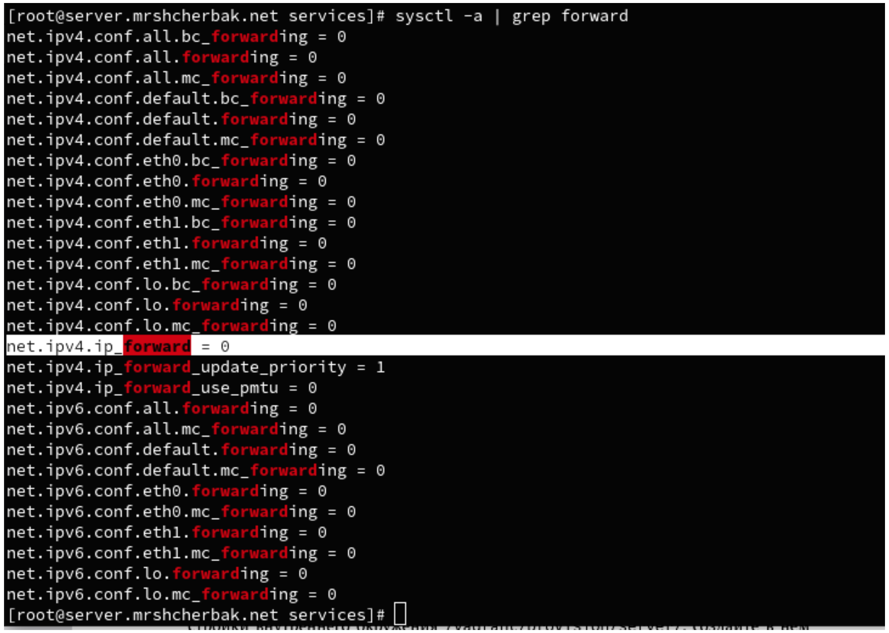


```
[root@server.mrshcherbak.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
```



```
[root@client.mrshcherbak.net ~]# ssh -p 2022 mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Web console: https://server.mrshcherbak.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Nov 23 21:49:44 2023 from 192.168.1.30
[mrshcherbak@server.mrshcherbak.net ~]$ 
```

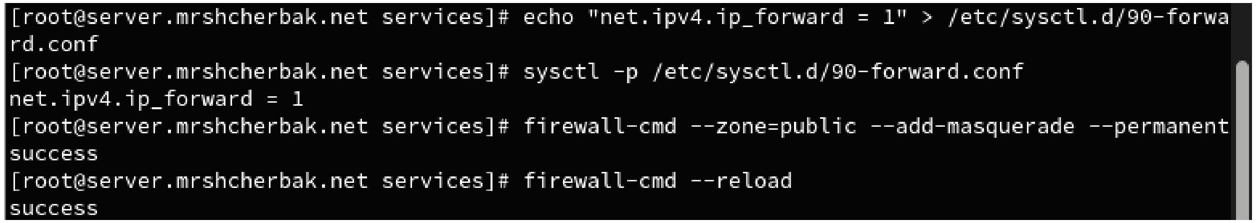
Настройка Port Forwarding и Masquerading



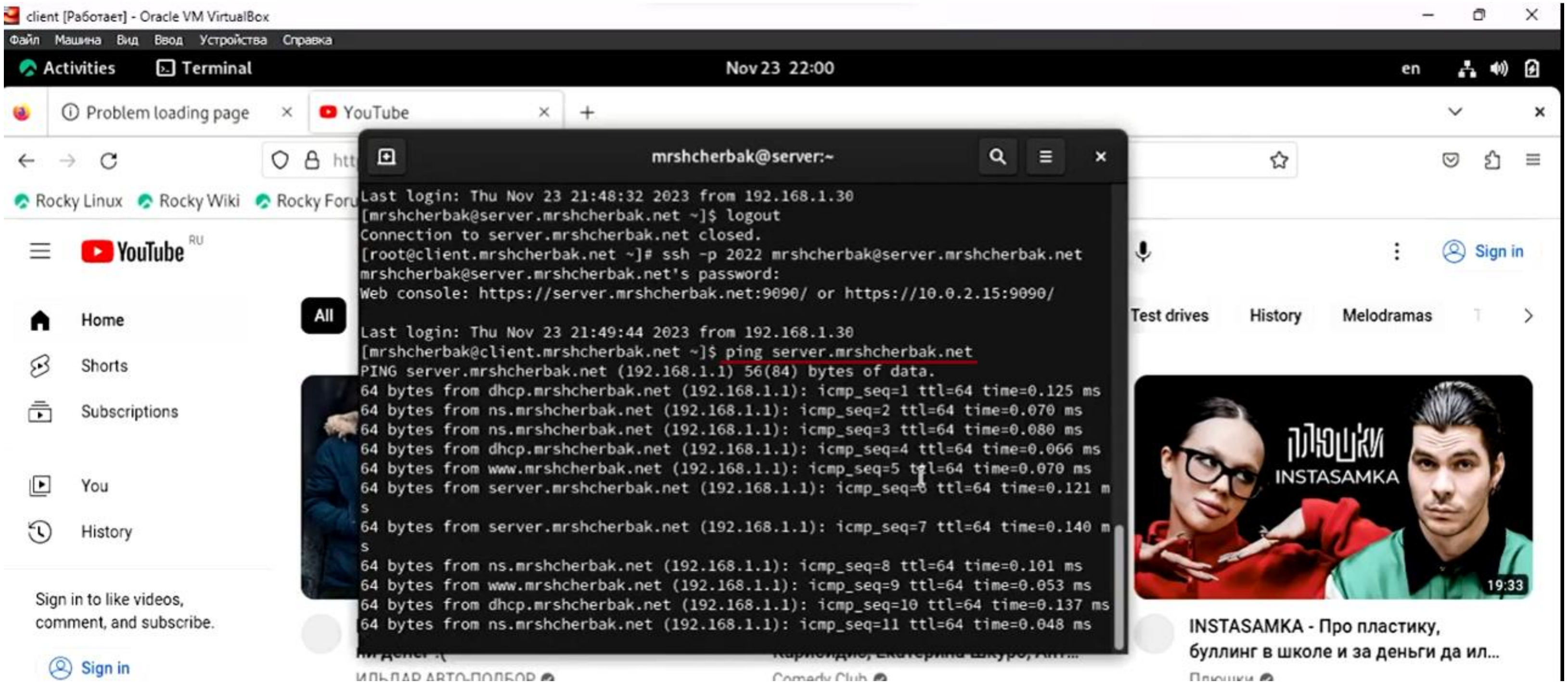
```
[root@server.mrshcherbak.net services]# sysctl -a | grep forward
net.ipv4.conf.all.bc_forwarding = 0
net.ipv4.conf.all.forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.default.bc_forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.eth0.bc_forwarding = 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.mrshcherbak.net services]# 
```

Возможность перенаправления IPv4-пакетов в ядре системы не активирована

Включила перенаправление IPv4-пакетов и маскарадинг на сервере

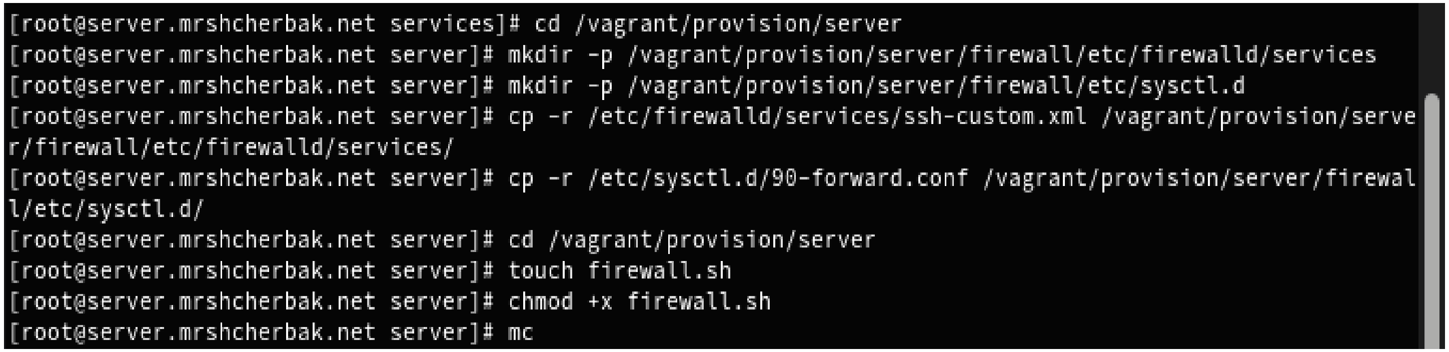


```
[root@server.mrshcherbak.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forwa
rd.conf
[root@server.mrshcherbak.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.mrshcherbak.net services]# firewall-cmd --zone=public --add-masquerade --permanent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



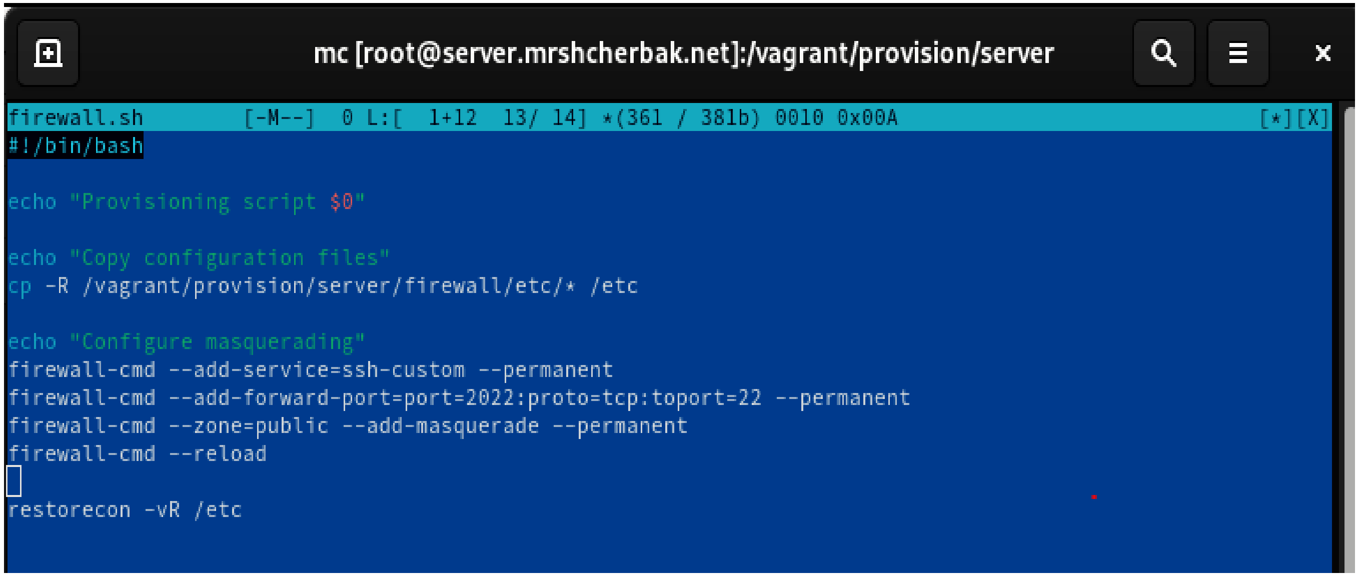
```
Last login: Thu Nov 23 21:48:32 2023 from 192.168.1.30
[mrshcherbak@server.mrshcherbak.net ~]$ logout
Connection to server.mrshcherbak.net closed.
[root@client.mrshcherbak.net ~]# ssh -p 2022 mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Web console: https://server.mrshcherbak.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Nov 23 21:49:44 2023 from 192.168.1.30
[mrshcherbak@client.mrshcherbak.net ~]$ ping server.mrshcherbak.net
PING server.mrshcherbak.net (192.168.1.1) 56(84) bytes of data.
64 bytes from dhcp.mrshcherbak.net (192.168.1.1): icmp_seq=1 ttl=64 time=0.125 ms
64 bytes from ns.mrshcherbak.net (192.168.1.1): icmp_seq=2 ttl=64 time=0.070 ms
64 bytes from ns.mrshcherbak.net (192.168.1.1): icmp_seq=3 ttl=64 time=0.080 ms
64 bytes from dhcp.mrshcherbak.net (192.168.1.1): icmp_seq=4 ttl=64 time=0.066 ms
64 bytes from www.mrshcherbak.net (192.168.1.1): icmp_seq=5 ttl=64 time=0.070 ms
64 bytes from server.mrshcherbak.net (192.168.1.1): icmp_seq=6 ttl=64 time=0.121 m
s
64 bytes from server.mrshcherbak.net (192.168.1.1): icmp_seq=7 ttl=64 time=0.140 m
s
64 bytes from ns.mrshcherbak.net (192.168.1.1): icmp_seq=8 ttl=64 time=0.101 ms
64 bytes from www.mrshcherbak.net (192.168.1.1): icmp_seq=9 ttl=64 time=0.053 ms
64 bytes from dhcp.mrshcherbak.net (192.168.1.1): icmp_seq=10 ttl=64 time=0.137 ms
64 bytes from ns.mrshcherbak.net (192.168.1.1): icmp_seq=11 ttl=64 time=0.048 ms
```

Внесение изменений в настройки внутреннего окружения виртуальной машины



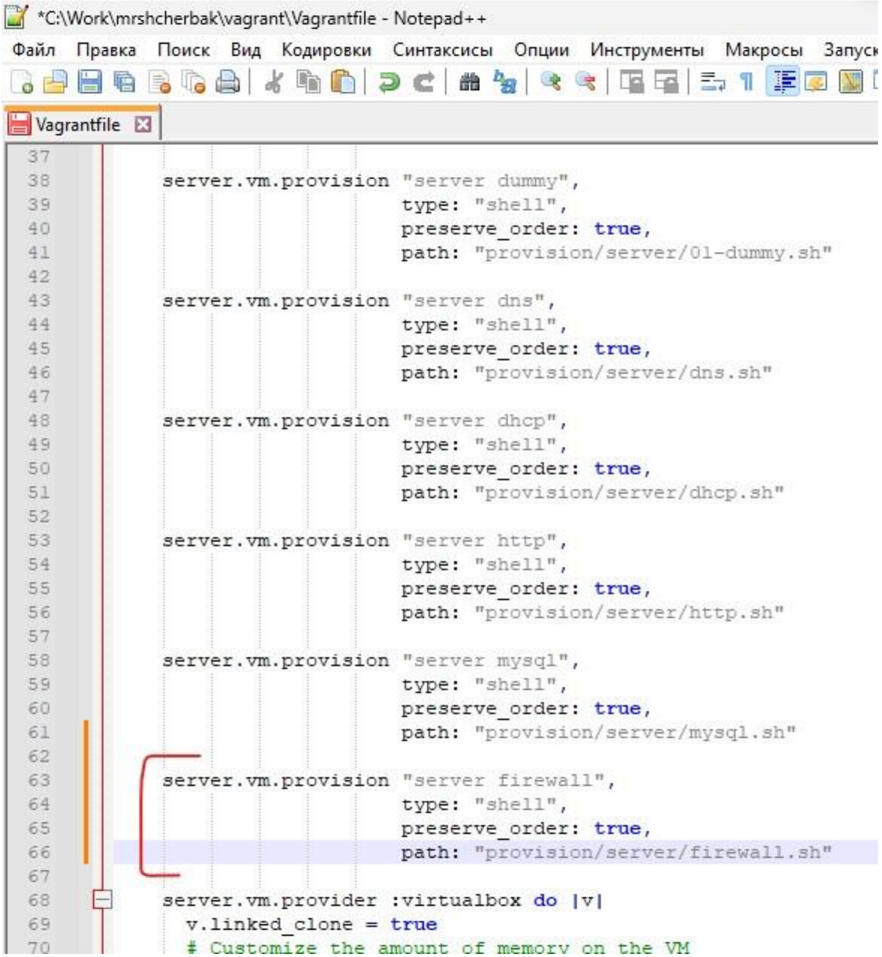
```
[root@server.mrshcherbak.net services]# cd /vagrant/provision/server
[root@server.mrshcherbak.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server.mrshcherbak.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.mrshcherbak.net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

Редактирование файла firewall.sh



mc [root@server.mrshcherbak.net]:/vagrant/provision/server

```
firewall.sh      [-M--]  0 L:[  1+12  13/ 14] *(361 / 381b) 0010 0x00A                    [*][X]
#!/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
```



```

    server.vm.provision "server dummy",
                        type: "shell",
                        preserve_order: true,
                        path: "provision/server/01-dummy.sh"

    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
      # Customize the amount of memory on the VM
```

Вывод: таким образом, в ходе выполнения л/р №7 я получила навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.