РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

Отчет лабораторной работы 7

Дисциплина: Администрирование сетевых подсистем

Студент: Астахова Марина

Группа: НПИбд-02-23

Тема: Расширенные настройки межсетевого экрана

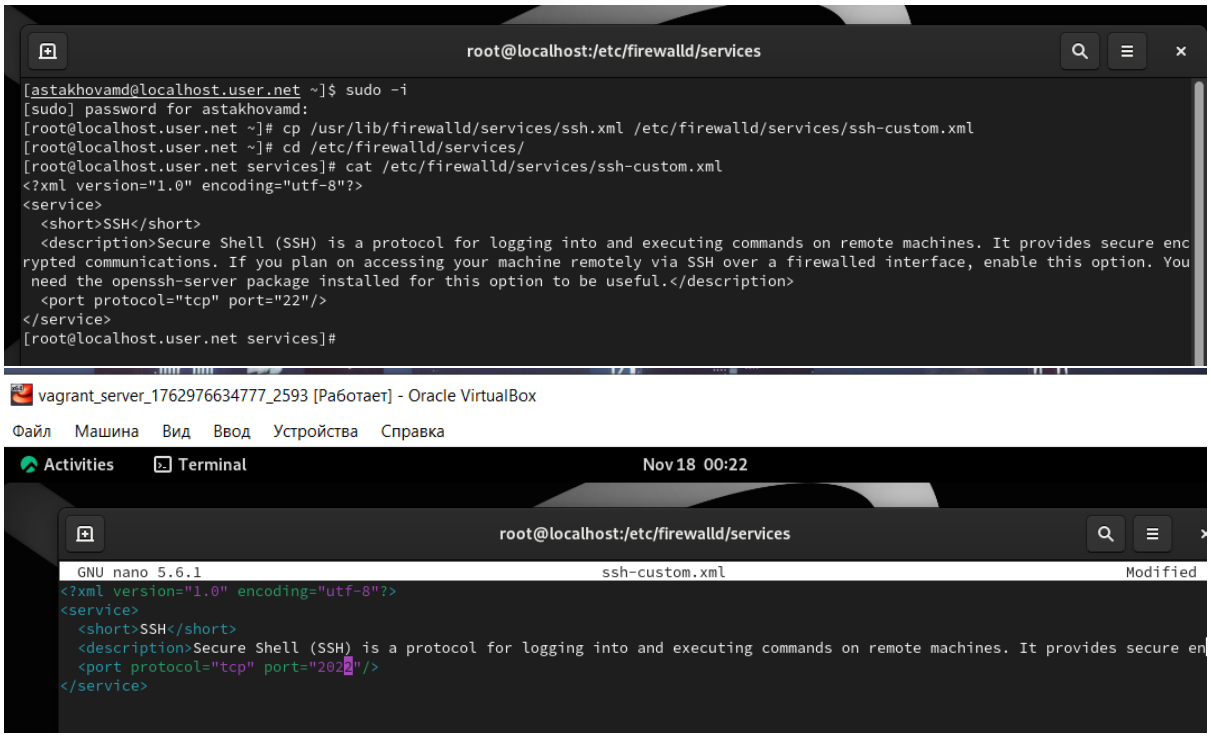
7.1. Цель работы.

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

7.2. Выполнение работы

1. Настройте межсетевой экран виртуальной машины server для доступа к серверу по протоколу SSH не через22-й порт, а через порт 2022. Создание пользовательской службы firewalld.

Обновили порты и заменили на порт 2022



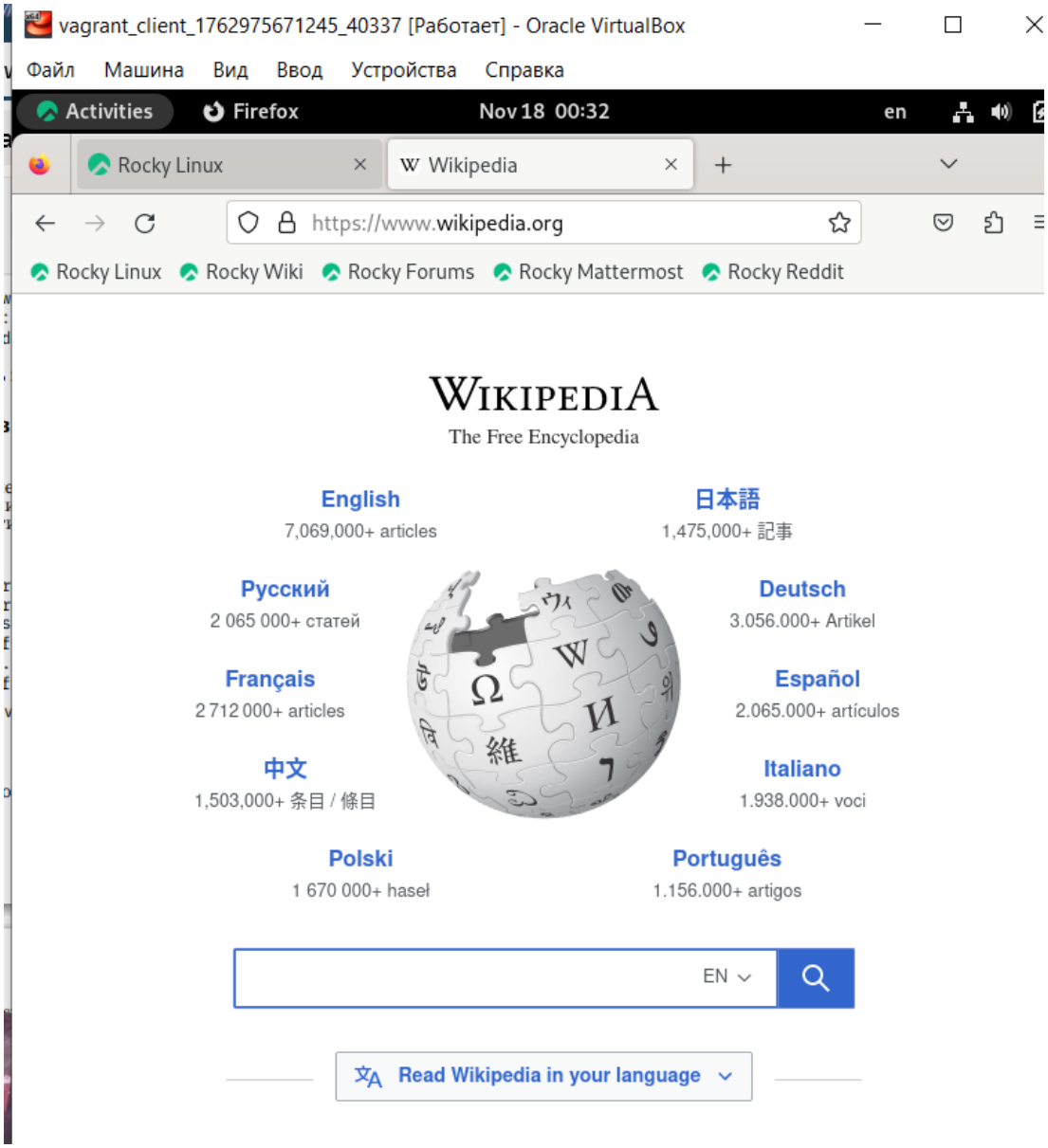
```
[root@localhost.user.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-client
 bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ce
ph ceph-exporter 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-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server f
inger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client gangl
ia-master git gpsd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target
 isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-contro
l-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-client llmnr-tcp
llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios
-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole ple
x pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv p
tp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rootd 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 snmptrap spideroak-lansync spotify-sync squ
id ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile3
8 tinc tor-socks transmission-client upnp-client vdsm vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discove
ry-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-se
rver zerotier
[root@localhost.user.net services]#
```

```
[root@localhost.user.net services]# firewall-cmd --reload
success
[root@localhost.user.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-client
 bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ce
ph ceph-exporter 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-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server f
inger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client gangl
ia-master git gpsd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target
 isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-contro
l-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-client llmnr-tcp
llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios
-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole ple
x pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv p
tp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rootd 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 snmptrap spideroak-lansync spotify-sync squ
id ssdp ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle
 tftp tile38 tinc tor-socks transmission-client upnp-client vdsm 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-agen
t zabbix-server zerotier
[root@localhost.user.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@localhost.user.net services]#
```

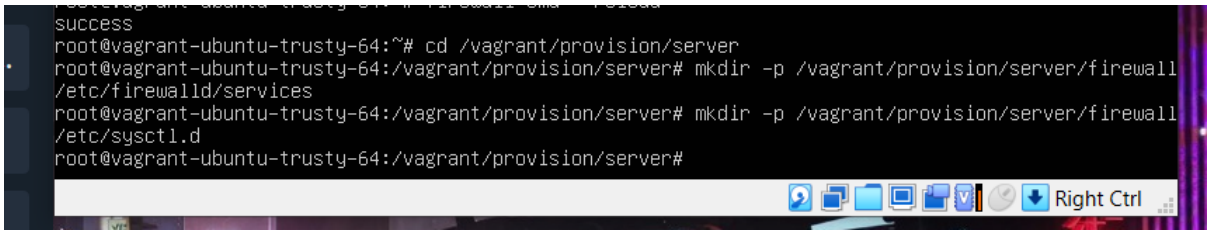
```
 ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-
t zabbix-server zerotier
[root@localhost.user.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@localhost.user.net services]# firewall-cmd --add-service=ssh-custom
success
[root@localhost.user.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@localhost.user.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@localhost.user.net services]# firewall-cmd --reload
success
[root@localhost.user.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
[root@localhost.user.net services]# ssh -p 2022 astakhovamd@server.astakhovamd.net
```

```
[root@localhost.user.net services]# systemctl start sshd
[root@localhost.user.net services]# systemctl enable sshd
[root@localhost.user.net services]#     grep Port /etc/ssh/sshd_config

#Port 22
#GatewayPorts no
[root@localhost.user.net services]#     systemctl restart sshd

[root@localhost.user.net services]# firewall-cmd --zone=public --add-port=2022/tcp --permanent
success
[root@localhost.user.net services]# firewall-cmd --reload
success
[root@localhost.user.net services]#     ss -tulpen | grep 2022

[root@localhost.user.net services]#
```

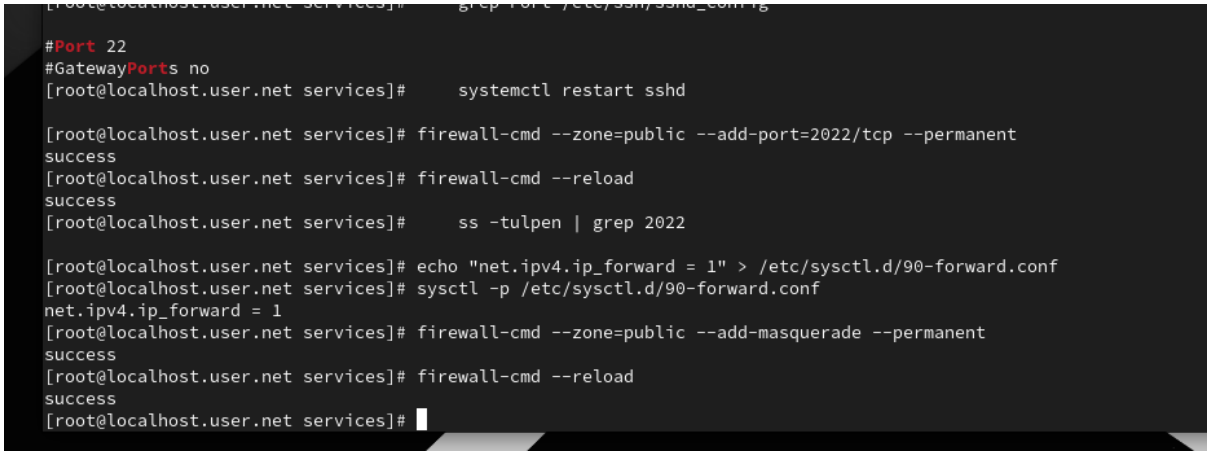
Проверили после этого доступ в интернет с client



Добавили в службы FirewallD и сделали доступным в реальном времени



2. Настройте маскарадинг на виртуальной машине server для организации доступа клиента к сети Интернет. Настройка Port Forwarding и Masquerading.

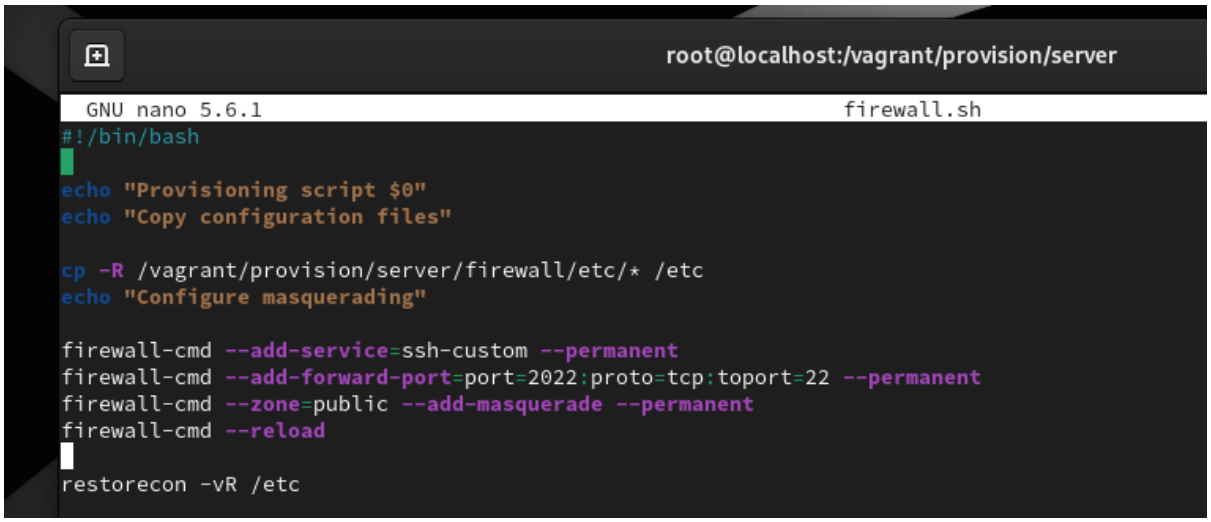


3. Напишите скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внести изменения в Vagrantfile. Внесение изменений в настройки внутреннего окружения виртуальной машины

Создаем файл firewall.sh в каталоге

```
[root@localhost.user.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@localhost.user.net services]# firewall-cmd --reload
success
[root@localhost.user.net services]# cd /vagrant/provision/server
[root@localhost.user.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@localhost.user.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@localhost.user.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/se
rvices/
[root@localhost.user.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d/
[root@localhost.user.net server]# cd /vagrant/provision/server
[root@localhost.user.net server]# touch firewall.sh
[root@localhost.user.net server]# chmod +x firewall.sh
[root@localhost.user.net server]#
```

Добавляем в файл скрипт



В vagrantfile добавляем изменения для закрепления изменений

```
                    path: "provision/server/http.sh"
  end

 server.vm.provision "server mysql",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/server/mysql.sh"
  end

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

7.3. Итог работы

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

7.4. Контрольные вопросы

1. *Где хранятся пользовательские файлы firewalld?*
   Пользовательские файлы конфигурации firewalld (например, для пользовательских зон, служб, политик) хранятся в директории /etc/firewalld/.
   i. ***Пользовательские зоны: /etc/firewalld/zones/***
   ii. ***Пользовательские службы: /etc/firewalld/services/***

2. *Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?*

   В XML-файл пользовательской службы (например, mycustomservice.xml), внутри тегов ..., нужно добавить следующую строку:
   <port protocol="tcp" port="2022"/>

3. *Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере?*
   Для перечисления всех доступных служб firewalld используется команда:
   firewall-cmd --get-services

4. *В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)?*

   NAT (Network Address Translation) — это общий термин для технологии, которая изменяет IP-адреса и/или номера портов в заголовках IP-пакетов при их прохождении через маршрутизатор или брандмауэр.

Существуют два основных типа:

1. **SNAT (Source NAT):** Изменяет исходный IP-адрес пакета.
2. **DNAT (Destination NAT):** Изменяет IP-адрес назначения пакета.

Маскарадинг — это динамический SNAT, который автоматически определяет внешний IP-адрес для исходящих соединений. NAT — это более широкое понятие, включающее как статические, так и динамические преобразования адресов, а также преобразования адресов назначения.

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 --zone=public --add-forward port=port=4404:proto=tcp:toport=22:toaddr=10.0.0.10 --permanent***
- ***sudo firewall-cmd –reload***

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

- ***sudo firewall-cmd --zone=public --add-masquerade --permanent***
- ***sudo firewall-cmd --reload***