

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных
наук Кафедра прикладной информатики и теории
вероятностей**

ОТЧЕТ

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №
7**

**ДИСЦИПЛИНА: АДМИНИСТРИРОВАНИЕ СЕТЕВЫХ
ПОДСИСТЕМ**

Студент: Яссин оулед

салеи

НПИбд-02-20

МОСКВА 2022 г.

Цель работы

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

Последовательность выполнения работы

1. Создание пользовательской службы firewalld

1. На основе существующего файла описания службы ssh создайте файл с собственным описанием: `cp /usr/lib/firewalld/services/ssh.xml ↔ /etc/firewalld/services/ssh-custom.xml`
`cd /etc/firewalld/services/`

```
[root@server.yassine.net ~]# cd /etc/firewalld/services/
[root@server.yassine.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.yassine.net ~]# cd /etc/firewalld/services/
[root@server.yassine.net services]#
```

2. Посмотрите содержимое файла службы: `cat /etc/firewalld/services/ssh-custom.xml` В отчёте построчно прокомментируйте принцип синтаксиса файла описания службы.

```
[root@server.yassine.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>
[root@server.yassine.net services]#
```

3. Откройте файл описания службы на редактирование и замените порт 22 на новый порт (2022): В этом же файле скорректируйте описание службы для демонстрации, что это модифицированный файл службы.

```
root@server:/etc/firewalld/services  x  root@server:~  x
<?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="2022"/>
</service>
~
~
~
~
~
```

4. Просмотрите список доступных FirewallD служб: `firewall-cmd --get-services` Обратите внимание, что новая служба ещё не отображается в списке.

```
[root@server.yassine.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd audit bacula ba
ula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon
fengine cockpit collectd condor-collector ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker
registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-prox
freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client gangl
a-master git grafana gre high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-ta
get isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver
ube-control-plane kube-controller-manager kube-scheduler kubelet-worker ldap ldaps libvirt libvirt-tls
lightning-network llmnr managesieve matrix mdns memcache minidlina mongodb mosh mountd mqtt mqtt-tls ms-w
t mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storage
onsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus pr
xy-dhcp ptp pulseaudio 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 snmptrap
spideroak-lansync spotify-sync squid sssd ssh steam-streaming svdrp svn syncthing syncthing-gui synergy
syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsd vnc-s
rver wbem-http wbem-https wireguard wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zab
ix-agent zabbix-server
[root@server.yassine.net services]#
```

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` Убедитесь, что созданная вами служба отображается в списке доступных для FirewallD служб, но не активирована.

```
[root@server.yassine.net services]# firewall-cmd --reload
success
[root@server.yassine.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd audit bacula ba
ula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon
fengine cockpit collectd condor-collector ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker
registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-prox
freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client gangl
a-master git grafana gre high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-ta
get isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver
ube-control-plane kube-controller-manager kube-scheduler kubelet-worker ldap ldaps libvirt libvirt-tls
lightning-network llmnr managesieve matrix mdns memcache minidlina mongodb mosh mountd mqtt mqtt-tls ms-w
t mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storage
onsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus pr
xy-dhcp ptp pulseaudio 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 snmptrap
spideroak-lansync spotify-sync squid sssd ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-
ui synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client
vdsd vnc-server wbem-http wbem-https wireguard wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp
server zabbix-agent zabbix-server
[root@server.yassine.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.yassine.net services]#
```

6. Добавьте новую службу в FirewallD и выведите на экран список активных служб: `firewall-cmd --add-service=ssh-custom firewall-cmd --list-services`

```
firewall-cmd: error: unrecognized arguments: --add-service=ssh-custom
[root@server.yassine.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.yassine.net services]# firewall-cmd --lost-services
usage: see firewall-cmd man page
firewall-cmd: error: unrecognized arguments: --lost-services
[root@server.yassine.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.yassine.net services]#
```

2-Перенаправление портов

1. Организуйте на сервере переадресацию с порта 2022 на порт 22: `firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22`

```
cockpit dhcp dnscv6-client dns http https ssh ssh-custom
[root@server.yassine.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
Warning: ALREADY_ENABLED: '2022:tcp:22:' already in 'public'
success
[root@server.yassine.net services]#
```

2. На клиенте попробуйте получить доступ по SSH к серверу через порт 2022: `ssh -p 2022 user@server.user.net` (вместо user укажите свой логин).

```
[yassine@client.yassine.net ~]$ ssh -p 2022 yassine@server.yassine.net
The authenticity of host '[server.yassine.net]:2022 ([192.168.1.1]:2022)' ca
be established.
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0qNzuP7z0xlg0qvGhkHxMkw2sQdb1
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.yassine.net]:2022' (ED25519) to the list
known hosts.
yassine@server.yassine.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Nov 28 10:41:25 2022
[yassine@server.yassine.net ~]$

[root@server.yassine.net services]# ssh -p 2022 yassine@server.yassine.net
ssh: connect to host server.yassine.net port 2022: Connection timed out
[root@server.yassine.net services]#
```

3. Настройка Port Forwarding и Masquerading

1. На сервере посмотрите, активирована ли в ядре системы возможность перенаправления IPv4-пакетов: `sysctl -a | grep forward`

```
[root@server.yassine.net services]# cd
[root@server.yassine.net ~]# 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
```

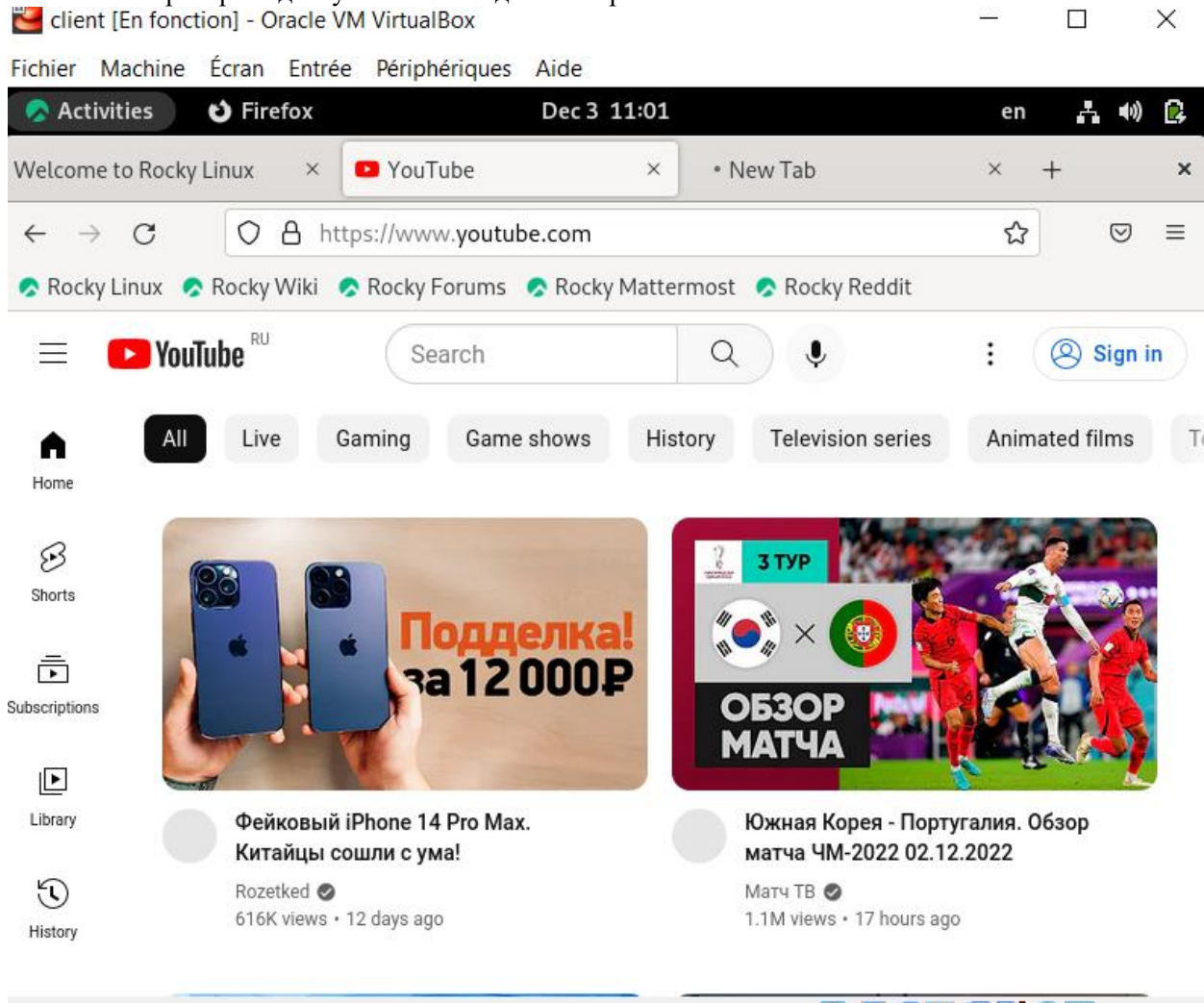
2. Включите перенаправление IPv4-пакетов на сервере: `echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf sysctl -p /etc/sysctl.d/90-forward.conf`

```
[root@server.yassine.net ~]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.yassine.net ~]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.yassine.net ~]#
```

- Включите маскрадинг на сервере: `firewall-cmd --zone=public --add-masquerade --permanent`
`firewall-cmd --reload`

```
[root@server.yassine.net ~]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.yassine.net ~]# firewall-cmd --reload
success
[root@server.yassine.net ~]#
```

- На клиенте проверьте доступность выхода в Интернет



4. Внесение изменений в настройки внутреннего окружения виртуальной машины

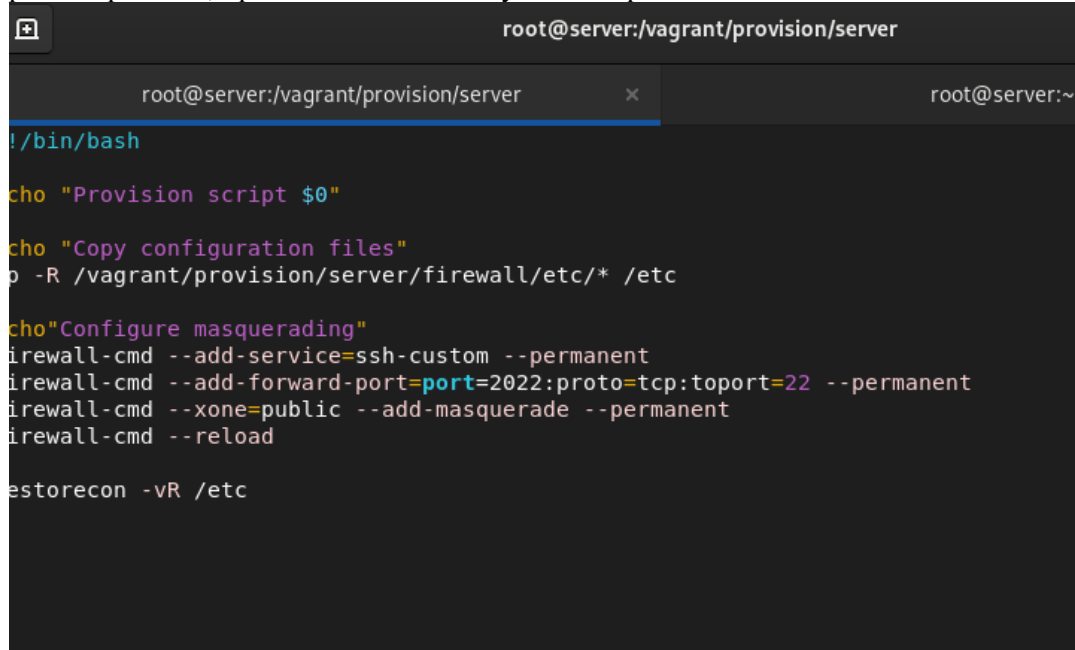
- На виртуальной машине `server` перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создайте в нём каталог `firewall`, в который поместите в соответствующие подкаталоги конфигурационные файлы FirewallD: `cd /vagrant/provision/server mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services 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/`

```

[root@server.yassine.net ~]# cd /vagrant/provision/server
[root@server.yassine.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server.yassine.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.yassine.net server]# cp -r /etc/firewalld/services/ssh-custom.xml/vagrant/provision/server/
firewall/etc/firewalld/services/
cp: missing destination file operand after '/etc/firewalld/services/ssh-custom.xml/vagrant/provision/server/
firewall/etc/firewalld/services/'
Try 'cp --help' for more information.
[root@server.yassine.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server
/vagrant/provision/server/firewall/etc/firewalld/services/
[root@server.yassine.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall
/vagrant/provision/server/firewall/etc/sysctl.d/
[root@server.yassine.net server]#

```

- В каталоге /vagrant/provision/server создайте файл firewall.sh: `cd /vagrant/provision/server touch firewall.sh chmod +x firewall.sh` Открыв его на редактирование, пропишите в нём следующий скрипт:



```

root@server:~
root@server:~/vagrant/provision/server
root@server:~/vagrant/provision/server
#!/bin/bash

echo "Provision 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

systemctl restart firewalld.service
systemctl enable firewalld.service
systemctl restart storecon -vR /etc

```

- Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера: `server.vm.provision "server firewall", type: "shell", preserve_order: true, path: "provision/server/firewall.sh"`

```

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

```

ВЫВОД

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