

Отчет по лабораторной работе № 7.  
Расширенные настройки межсетевого экрана

Данила Стариков  
НПИбд-02-22

2024

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>3</b>
<b>2</b>	<b>Выполнение работы</b>	<b>4</b>
2.1	Создание пользовательской службы firewalld . . . . .	4
2.2	Перенаправление портов . . . . .	7
2.3	Настройка Port Forwarding и Masquerading . . . . .	7
2.4	Внесение изменений в настройки внутреннего окружения виртуальной машины . . . . .	9
<b>3</b>	<b>Ответы на контрольные вопросы</b>	<b>11</b>
<b>4</b>	<b>Выводы</b>	<b>12</b>

# 1 Цель работы

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

## 2 Выполнение работы

### 2.1 Создание пользовательской службы firewalld

1. Загрузили операционную систему и перешли в рабочий каталог с проектом:

```
cd ~/tmp/dastarikov/vagrant/
```

2. Запустили виртуальную машину server:

```
make server-up
```

3. На виртуальной машине server вошли под своимк пользователем и открыли терминал. Перешли в режим суперпользователя:

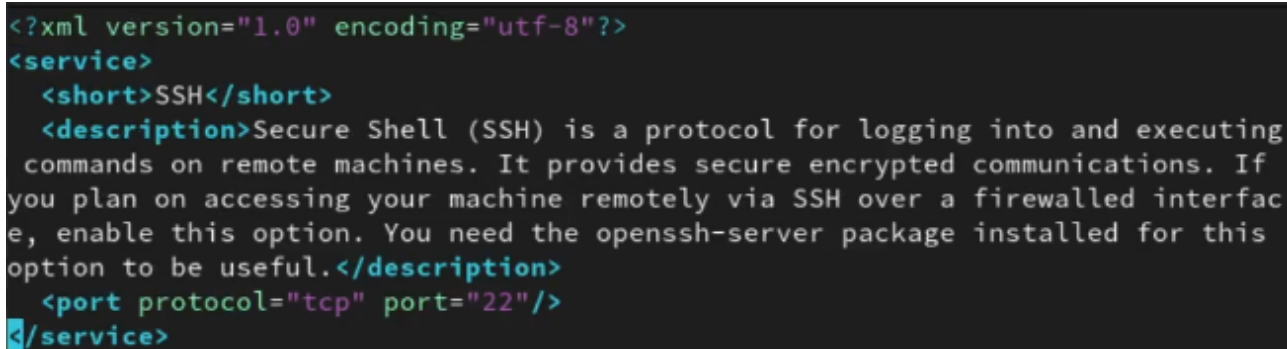
```
sudo -i
```

4. На основе существующего файла описания службы ssh создали файл с собственным описанием:

```
cp /usr/lib/firewalld/services/ssh.xml  
→ /etc/firewalld/services/ssh-custom.xml  
cd /etc/firewalld/services/
```

5. Посмотрели содержимое файла службы (Рис. 1):

```
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 interfac  
  e, enable this option. You need the openssh-server package installed for this  
  option to be useful.</description>  
  <port protocol="tcp" port="22"/>  
</service>
```

Рис. 1: Содержимое файла ssh.xml по умолчанию

6. Открыли файл описания службы на редактирование и заменили порт 22 на новый порт (2022):

```
<port protocol="tcp" port="2022"/>
```

Скорректировали описание службы, чтобы отметить, что она была изменена.

7. Просмотрели список доступных FirewallD служб (Рис. 2):

```
firewall-cmd --get-services
```

```
[root@server.dastarikov.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 b
itcoin-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 d
hcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticse
arch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps fre
eipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-
availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isn
s jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver ku
be-control-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 k
ubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-
udp managesieve matrix mdns memcache minidlna mongod mosh mountd mqtt mqtt-tls ms-wbt mssql murmu
r mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imag
eio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresq
l privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetma
ster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba sa
mba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptra
p spideroak-lansync spotify-sync squid ssdp ssh 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-disco
very-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local
xmpp-server zabbix-agent zabbix-server zerotier
```

Рис. 2: Список доступных служб.

Новая служба ещё не отображается в списке.

8. Перегрузили правила межсетевого экрана с сохранением информации о состоянии и вновь вывели на экран список служб, а также список активных служб (Рис. 3):

```
firewall-cmd --reload
firewall-cmd --get-services
firewall-cmd --list-services
```

```
[root@server.dastarikov.net services]# firewall-cmd --reload
firewall-cmd --get-services
firewall-cmd --list-services
success
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 b
itcoin-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 d
hcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticse
arch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps fre
eipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-
availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isn
s jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver ku
be-control-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 k
ubelet-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 murmu
r mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imag
eio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresq
l privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetma
ster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba sa
mba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptra
p spideroak-lansync spotify-sync squid sssd ssh ssh-custom steam-streaming svdrp svn syncthing syn
cthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks tr
ansmission-client upnp-client vdsms vnc-server warpinator wbem-http wbem-https wireguard ws-discove
ry ws-discovery-client ws-discovery-tcp ws-discovery-udp wsmans wsmans xdmcp xmpp-bosh xmpp-client
xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
cockpit dhcp dhcpv6-client dns http https ssh
```

Рис. 3: Список доступных и активных служб после обновления.

Созданная служба ssh-custom отобразилась в списке доступных для FirewallD служб, но не активирована.

9. Добавили новую службу в FirewallD и вывели на экран список активных служб (Рис. 4):

```
firewall-cmd --add-service=ssh-custom
firewall-cmd --list-services
```

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

Рис. 4: Список активных служб после добавления ssh-custom.

10. Служба была успешно добавлена в список активных, далее перезагрузили правила межсетевого экрана с сохранением информации о состоянии (Рис. 5):

```
firewall-cmd --add-service=ssh-custom --permanent
firewall-cmd --reload
```

```
[root@server.dastarikov.net services]# firewall-cmd --add-service=ssh-custom --permanent
firewall-cmd --reload
success
success
```

Рис. 5: Сохранение информации о состоянии и перезагрузка службы firewalld.

## 2.2 Перенаправление портов

1. Организовали на сервере переадресацию с порта 2022 на порт 22 (Рис. 6):

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

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

Рис. 6: Успешное добавление переадресации с порта 2022 на порт 22.

2. На клиенте попробовали получить доступ по SSH к серверу через порт 2022 (Рис. 7):

```
ssh -p 2022 dastarikov@server.dastarikov.net
```

```
[dastarikov@client.dastarikov.net ~]$ ssh -p 2022 dastarikov@server.dastarikov.net
The authenticity of host '[server.dastarikov.net]:2022 ([192.168.1.1]:2022)' can't be established.
ED25519 key fingerprint is SHA256:wPNWR0dsR7WQ4jis0U7+9Wpt3obVIYN5cqrQNHuJ9gw.
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.dastarikov.net]:2022' (ED25519) to the list of known hosts.
dastarikov@server.dastarikov.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Oct 19 13:28:33 2024
[dastarikov@server.dastarikov.net ~]$ id
uid=1001(dastarikov) gid=1001(dastarikov) groups=1001(dastarikov),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 7: Получение доступа по SSH на клиенте.

## 2.3 Настройка Port Forwarding и Masquerading

1. На сервере посмотрели, активирована ли в ядре системы возможность перенаправления IPv4 пакетов (Рис. 8):

```
sysctl -a | grep forward
```

```
[root@server.dastarikov.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
```

Рис. 8: Список параметров, связанных с перенаправлением пакетов.

2. Включили перенаправление IPv4 пакетов на сервере (Рис. 9):

```
echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
sysctl -p /etc/sysctl.d/90-forward.conf
```

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

Рис. 9: Включение перенаправления IPv4 пакетов на сервере.

3. Включили маскардинг на сервере (Рис. 10):



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

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

Рис. 10: Включение маскарадинга на сервере.

4. На клиенте проверили доступность выхода в Интернет (Рис. 11).

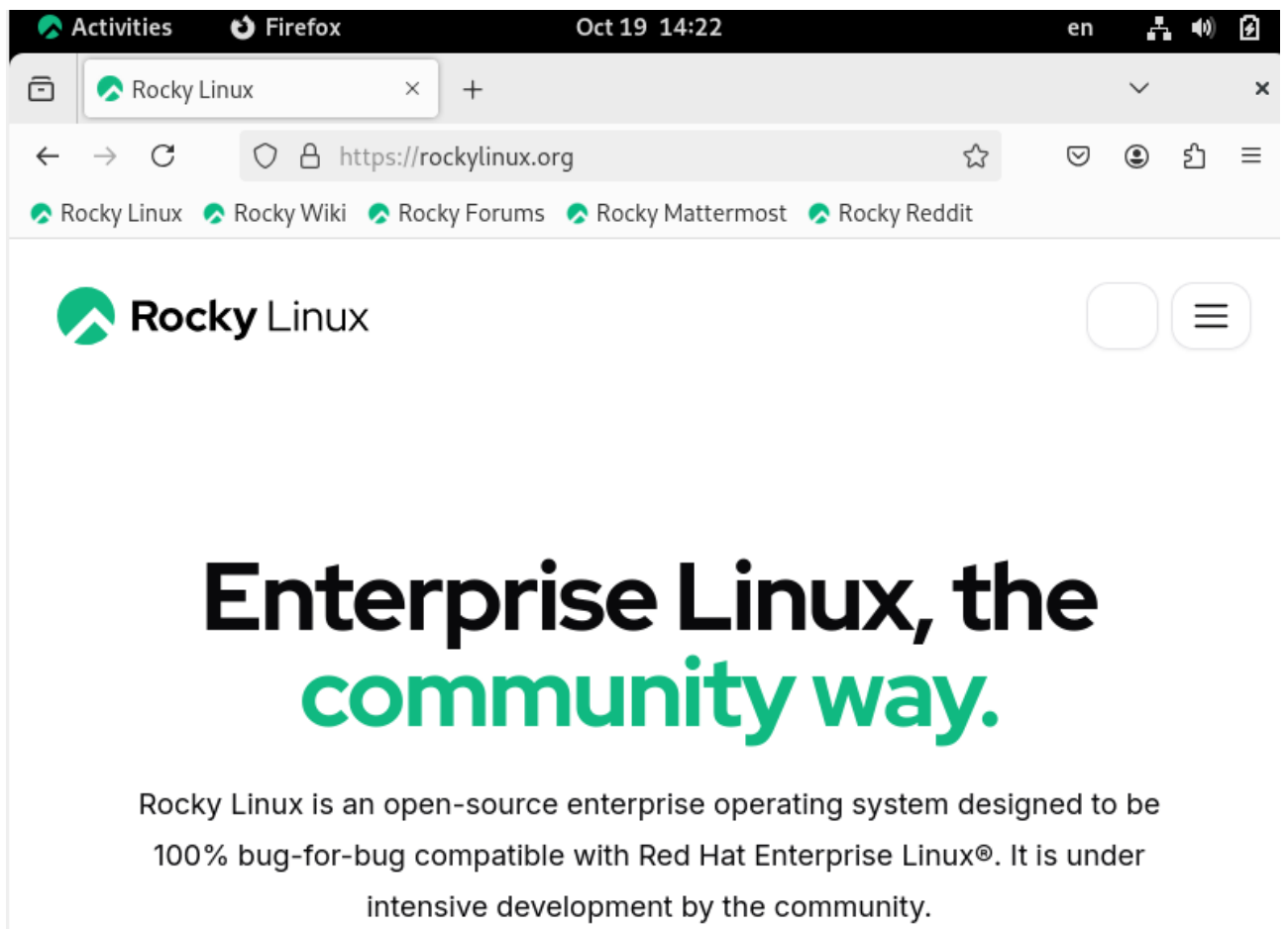


Рис. 11: Проверка доступности Интернета на клиенте.

## 2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине `server` перешли в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создайте в нём каталог `firewall`, в который поместили в соответствующие подкаталоги конфигурационные файлы `FirewallD` (Рис. 12):

```

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/

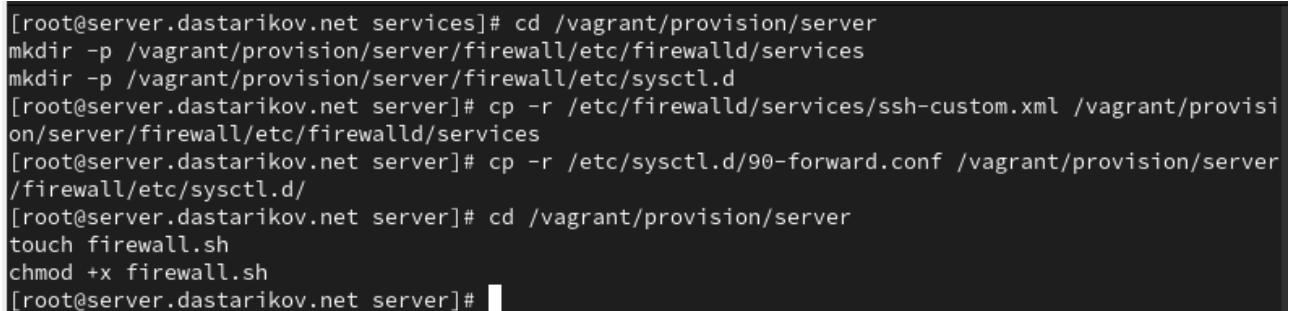
```

2. В каталоге /vagrant/provision/server создали файл firewall.sh (Рис. 12):

```

cd /vagrant/provision/server
touch firewall.sh
chmod +x firewall.sh

```



```

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

```

Рис. 12: Создание каталога с конфигурацией firewalld.

Прописал в нем следующий скрипт:

```

#!/bin/shell
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

```

3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавили в разделе конфигурации для сервера (Рис. 13):

```

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/firewall1.sh"
```

Рис. 13: Изменение Vagrantfile.

### 3 Ответы на контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?

Файлы хранятся в каталоге `/etc/firewalld/`.

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

Строку `<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)?

При трансляции сетевого адреса локальный IP-адрес преобразуется во внешний адрес, в то время как при маскарadingе локальный адрес заменяется на адрес связывающей машины.

5. Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10?

`firewall-cmd --add-forward-port=port=4404:proto=tcp:toaddr=10.0.0.10:toport=22`

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

`firewall-cmd --zone=public --add-masquerade`

## 4 Выводы

В результате выполнения лабораторной работы продолжили изучать настройки меж-  
сетевого экрана в Linux, настроили переадресацию портов и Masquerading.