

# Отчёт о лабораторной работе

Лабораторная работа 7

Мошаров Денис Максимович

## Содержание

### Цель работы

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

### Выполнение лабораторной работы

Запустим наш сервер через vagrant (рис. [-@fig:001]).

```
C:\Users\denis>cd C:\work_asp\dmmosharov\vagrant
C:\work_asp\dmmosharov\vagrant>vagrant up server
Bringing machine 'server' up with 'virtualbox' provider...
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: Clearing any previously set forwarded ports...
==> server: Clearing any previously set network interfaces...
==> server: Preparing network interfaces based on configuration...
      server: Adapter 1: nat
      server: Adapter 2: intnet
==> server: Forwarding ports...
      server: 22 (guest) => 2222 (host) (adapter 1)
==> server: Running 'pre-boot' VM customizations...
==> server: Booting VM...
==> server: Waiting for machine to boot. This may take a few minutes...
      server: SSH address: 127.0.0.1:2222
      server: SSH username: vagrant
      server: SSH auth method: password
```

Запуск сервера

Теперь зайдём под суперпользователем и скопируем файл описания службы ssh, создав его копию с названием ssh-custom.xml (рис. [-@fig:002]).

```
[root@server.dmmosharov.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.dmmosharov.net ~]# cd /etc/firewalld/services/
[root@server.dmmosharov.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 to have openssh-server package installed for this option to be useful.</description>
    <port protocol="tcp" port="22"/>
</service>
[root@server.dmmosharov.net services]#
```

Копирование конфигурационного файла

Теперь изменим его следующим образом. Основное отличие заключается в том, что порт для tcp назначен как 2022. Это XML-файл, который определяет пользовательскую службу для брандмауэра firewalld в Linux. Построчно опишем его:

Строка 1: xml version="1.0" encoding="utf-8"

Это стандартное объявление XML. Оно указывает, что файл использует версию XML 1.0 и кодировку символов UTF-8.

Строка 2: service

Это открывающий тег для корневого элемента. Он означает начало определения новой службы для firewalld.

Строка 3: short SSH-New /short

Этот тег задает короткое, удобное для чтения имя службы. В данном случае имя — “SSH-New”.

Строка 4: description Long SSH description /description

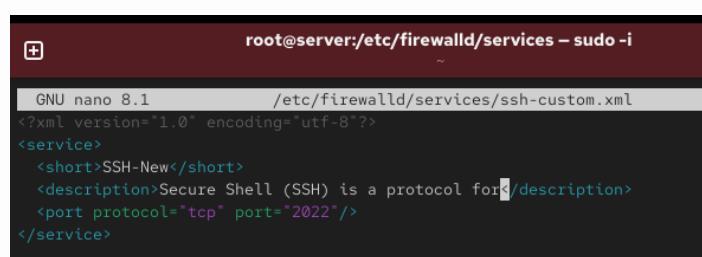
Здесь содержится более подробное описание службы. В этом примере используется текст “Long SSH description” (Длинное описание SSH).

Строка 5: port protocol="tcp" port="2022"

Это ключевая строка. Она определяет, что данная служба использует протокол tcp и слушает порт 2022. Когда эта служба будет активирована в firewalld, брандмаэр откроет порт 2022 для входящих TCP-соединений.

Строка 6: /service

Это закрывающий тег, который завершает определение службы. (рис. [-@fig:003]).



```
root@server:/etc/firewalld/services - sudo -i
GNU nano 8.1          /etc/firewalld/services/ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
    <short>SSH-New</short>
    <description>Secure Shell (SSH) is a protocol for</description>
    <port protocol="tcp" port="2022"/>
</service>
```

Редактирование файла /etc/firewalld/services/ssh-custom.xml

Выведем список доступных служб firewalld. Нашей созданной службы тут нет (рис. [-@fig:004]).

```
[root@server.dmmosharov.net services]# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp a
mqps anno-1602 anno-1800 apcupsd aseqnet audit ausweisapp2 bacula bacula-client bareos-di
rector bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoi
n-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilizat
ion-iv civilization-v cockpit collectd condor-collector cratedb ctdb dds dds-multicast dd
s-unicast dhcp dhcpcv6 dhcpcv6-client distcc dns dns-over-quic dns-over-tls docker-registry
docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger forem
an foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust f
tp galera ganglia-client ganglia-master git gpgsql grafana gre high-availability http http3
https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isn
s jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-api
server kube-control-plane kube-control-plane-secure kube-controller-manager kube-controll
er-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker
kubelite kubelite-readonly kubelite-worker ldap ldaps libvirt libvirt-tls lightning-network
llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft mindl
na nndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-f
or-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentel
emetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmweb
api pmwebapis pop3 pop3s postgresql privoxy prometheus-node-exporter proxy-dhc
p ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sen
tinel rooto rpe-bind rquodat rsh rsyncd rtsp salt-master samba samba-client samba-dc sane
settlers-history-collection sip sips slimevr slp smtp smtp-submission smtptp snmp snmppts
snmppts-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-tr
ansfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart s
vdrip svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls teln
et tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-clien
t vdsm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-discover
y-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-https wsman wsmans
xdmcpp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabb
ix-server zabbix-trapper zabbix-web-service zero-k zerotier
[root@server.dmmosharov.net services]#
```

### Список служб firewalld

Теперь перезапустим firewalld и снова выведем список доступных служб. Теперь наша служба отображается. Попробуем вывести список активных служб и увидим, что нашей службы пока в нём нет (рис. [-@fig:005]).

```
[root@server.dmmosharov.net services]# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp a
mqps anno-1602 anno-1800 apcupsd aseqnet audit ausweisapp2 bacula bacula-client bareos-di
rector bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoi
n-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilizat
ion-iv civilization-v cockpit collectd condor-collector cratedb ctdb dds dds-multicast dd
s-unicast dhcp dhcpcv6 dhcpcv6-client distcc dns dns-over-quic dns-over-tls docker-registry
docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger forem
an foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust f
tp galera ganglia-client ganglia-master git gpgsql grafana gre high-availability http http3
https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isn
s jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-api
server kube-control-plane kube-control-plane-secure kube-controller-manager kube-controll
er-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker
kubelite kubelite-readonly kubelite-worker ldap ldaps libvirt libvirt-tls lightning-network
llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft mindl
na nndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-f
or-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentel
emetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmweb
api pmwebapis pop3 pop3s postgresql privoxy prometheus-node-exporter proxy-dhc
p ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sen
tinel rooto rpe-bind rquodat rsh rsyncd rtsp salt-master samba samba-client samba-dc sane
settlers-history-collection sip sips slimevr slp smtp smtp-submission smtptp snmp snmppts
snmppts-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-tr
ansfer steam-streaming stellaris stronghold-crusader stun stuns submission sup
ertuxkart svdrip svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog sys
log-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns
upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery
ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-https ws
man wsmans xdmcpp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-ga
teway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
[root@server.dmmosharov.net services]# firewall-cmd --list-services
cockpit dhcp dhcpcv6-client dns http https ssh ssh-custom
[root@server.dmmosharov.net services]#
```

### Списки служб

Запустим созданную нами службу ssh-custom. Убедимся, что она запущена и находится в списке активных служб, после чего добавим её как постоянную службу, и перезагрузим firewalld (рис. [-@fig:006]).

```
[root@server.dmmosharov.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.dmmosharov.net services]# firewall-cmd --list-services
cockpit dhcp dhcpcv6-client dns http https ssh ssh-custom
[root@server.dmmosharov.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.dmmosharov.net services]# firewall-cmd --reload
success
[root@server.dmmosharov.net services]#
```

## Добавление службы как активной

С помощью firewalld настроим форвардинг портов с 2022 на 22 (рис. [-@fig:007]).

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

## Форвардинг портов

Попробуем с клиента подключиться по ssh к серверу, используя именно 2022 порт. Как видим, операция прошла успешно (рис. [-@fig:008]).

```
[root@server.dmmosharov.net services]# ssh -p 2022 dmmosharov@server.dmmosharov.net  
The authenticity of host '[server.dmmosharov.net]:2022 ([192.168.1.1]:2022)' can't be est  
ablished.  
ED25519 key fingerprint is SHA256:F8sRE0Cc3d3bq03xJrbnrCFDPDWDr/+seyPOj5DX9uI.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '[server.dmmosharov.net]:2022' (ED25519) to the list of known  
hosts.  
dmmosharov@server.dmmosharov.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Fri Jan 23 15:56:04 2026  
[dmmosharov@server.dmmosharov.net ~]$
```

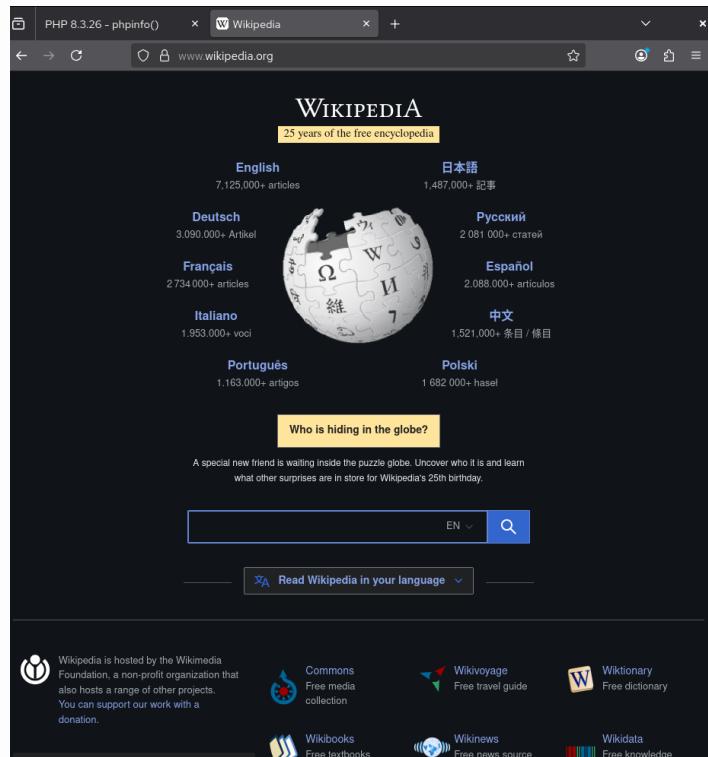
## Подключение по ssh

Проверим, включена ли в ядре опция перенаправления ipv4 пакетов. Как видим, переключатель стоит в положении 0. Запишем настройку net.ipv4.ip\_forward = 1 в файл конфигурации /etc/sysctl.d/90-forward.conf. После этого загружаем этот конфигурационный файл и включаем через firewall-cmd маскарадинг (рис. [-@fig:009]).

```
net.ipv4.conf.eth0.bc_forwarding = 0  
net.ipv4.conf.eth0.forwarding = 1  
net.ipv4.conf.eth0.mc_forwarding = 0  
net.ipv4.conf.eth1.bc_forwarding = 0  
net.ipv4.conf.eth1.forwarding = 1  
net.ipv4.conf.eth1.mc_forwarding = 0  
net.ipv4.conf.lo.bc_forwarding = 0  
net.ipv4.conf.lo.forwarding = 1  
net.ipv4.conf.lo.mc_forwarding = 0  
net.ipv4.ip_forward = 1  
net.ipv4.ip_forward_update_priority = 1  
net.ipv4.ip_forward_use_pmtu = 0  
sysctl: permission denied on key 'net.ipv4.tcp_fastopen_key'  
net.ipv6.conf.all.forwarding = 0  
net.ipv6.conf.all.mc_forwarding = 0  
sysctl: permission denied on key 'net.ipv6.conf.all.stable_secret'  
sysctl: permission denied on key 'net.ipv6.conf.default.stable_secret'  
net.ipv6.conf.default.forwarding = 0  
net.ipv6.conf.default.mc_forwarding = 0  
sysctl: permission denied on key 'net.ipv6.conf.eth0.stable_secret'  
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  
sysctl: permission denied on key 'net.ipv6.conf.eth1.stable_secret'  
net.ipv6.conf.lo.forwarding = 0  
net.ipv6.conf.lo.mc_forwarding = 0  
sysctl: permission denied on key 'net.ipv6.conf.lo.stable_secret'  
sysctl: permission denied on key 'vm.mmap_rnd_bits'  
sysctl: permission denied on key 'vm.mmap_rnd_compat_bits'  
sysctl: permission denied on key 'vm.stat_refresh'  
[dmmosharov@server.dmmosharov.net ~]$ echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-f  
orward.conf  
-bash: /etc/sysctl.d/90-forward.conf: Permission denied  
[dmmosharov@server.dmmosharov.net ~]$ sudo -i  
[sudo] password for dmmosharov:  
Sorry, try again.  
[sudo] password for dmmosharov:  
[root@server.dmmosharov.net ~]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward  
.conf  
[root@server.dmmosharov.net ~]# sysctl -p /etc/sysctl.d/90-forward.conf  
net.ipv4.ip_forward = 1  
[root@server.dmmosharov.net ~]# firewall-cmd --zone=public --add-masquerade --permanent  
success  
[root@server.dmmosharov.net ~]# firewall-cmd --reload  
success  
[root@server.dmmosharov.net ~]#
```

## Включение перенаправления и маскарадинга

Теперь с клиента попробуем зайти в сеть интернет. Как видим, интернет работает (рис. [-@fig:010]).



#### Проверка доступа в интернет

После этого сохраним все конфигурационные файлы в vagrant и создадим скрипт firewall.sh (рис. [-@fig:011]).

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

#### Сохранение конфигурации vagrant

В созданном скрипте firewall.sh пропишем следующие строки для настройки ssh и маскарадинга (рис. [-@fig:012]).

```
GNU nano 8.1                               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
```

#### firewall.sh

И запишем в vagrantfile автозагрузку этого скрипта (рис. [-@fig:013]).

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

Vagrantfile

## Выводы

В результате выполнения лабораторной работы были получены навыки работы с фаерволом и настройкой форвардинга и маскарадинга