Лабораторная работа

Номер 7

Мошаров Д. М.

01 января 1970

Российский университет дружбы народов, Москва, Россия

Информация

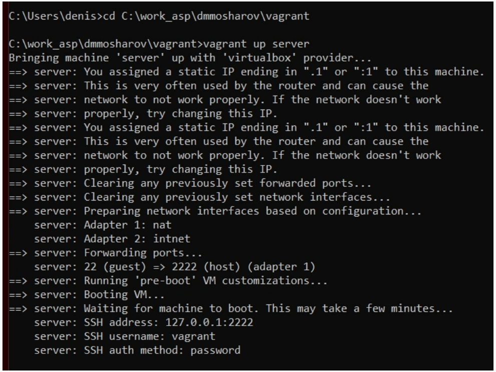
Докладчик

- Мошаров Денис Максимович
- Студент
- Российский университет дружбы народов

Цель работы

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

Запуск сервера

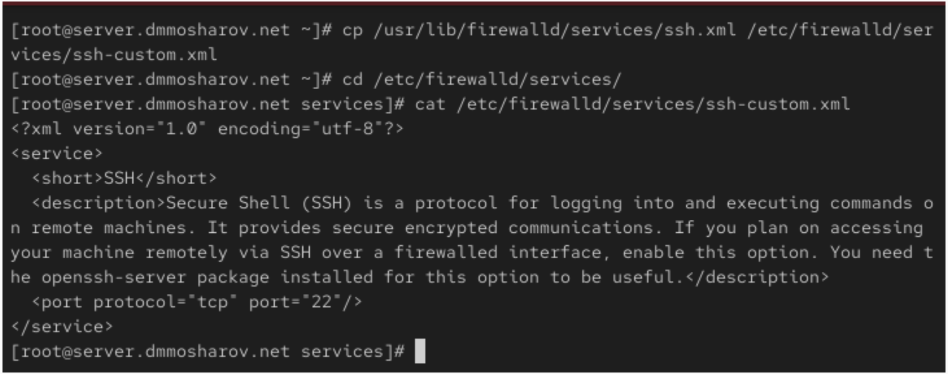


```
C:\Users\denis>cd C:\work_asp\dmmosharov\vagrant

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
```

Рис. 1: Запуск сервера

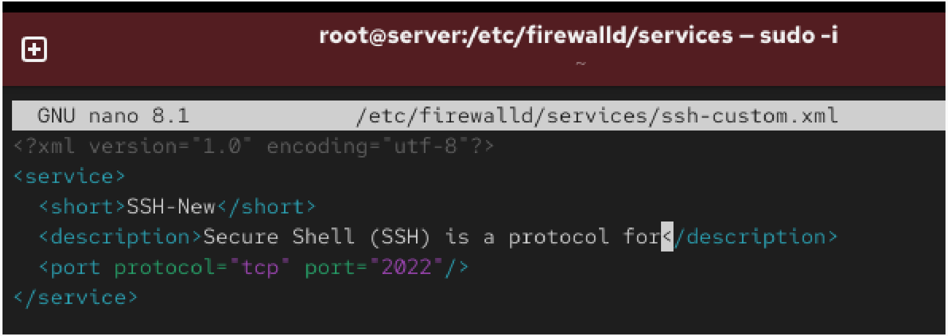
Копирование конфигурационного файла



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

Рис. 2: Копирование конфигурационного файла

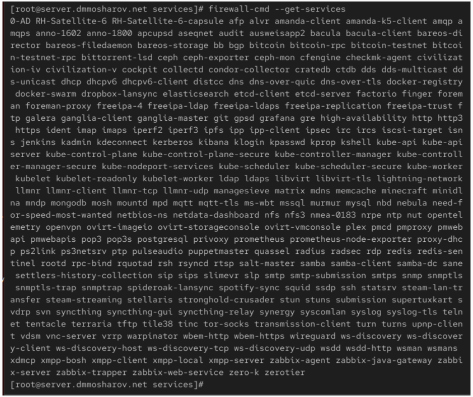
Редактирование файла /etc/firewalld/services/ssh-custom.xml



```
 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>
```

Рис. 3: Редактирование файла /etc/firewalld/services/ssh-custom.xml

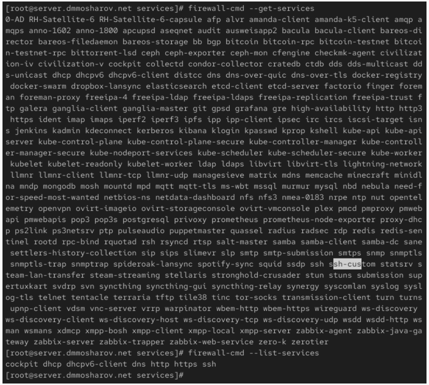
Список служб firewalld



```
[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 dhcpv6 dhcpv6-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 gpsd 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
 kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network
 llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidl
na mndp 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 prometheus-node-exporter proxy-dhc
p ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sen
tinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane
 settlers-history-collection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls
 snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-tr
ansfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart s
vdrp 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-http wsman wsmans
xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbi
x-server zabbix-trapper zabbix-web-service zero-k zerotier
[root@server.dmmosharov.net services]#
```

Рис. 4: Список служб firewalld

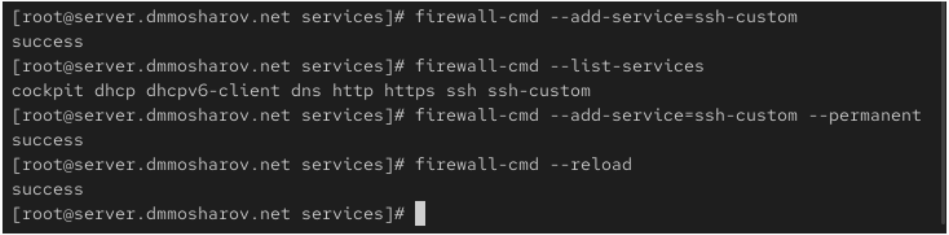
Списки служб



```
[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 dhcpv6 dhcpv6-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 gpsd 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
 kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network
 llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidl
na mndp 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 prometheus-node-exporter proxy-dhc
p ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sen
tinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane
 settlers-history-collection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls
 snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom statsrv s
team-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission sup
ertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog sysl
og-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-http ws
man wsmans xdmcp 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 dhcpv6-client dns http https ssh
[root@server.dmmosharov.net services]#
```

Рис. 5: Списки служб

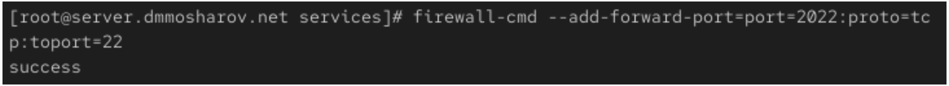
Добавление службы как активной



```
[root@server.dmmosharov.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.dmmosharov.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-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]# 
```

Рис. 6: Добавление службы как активной

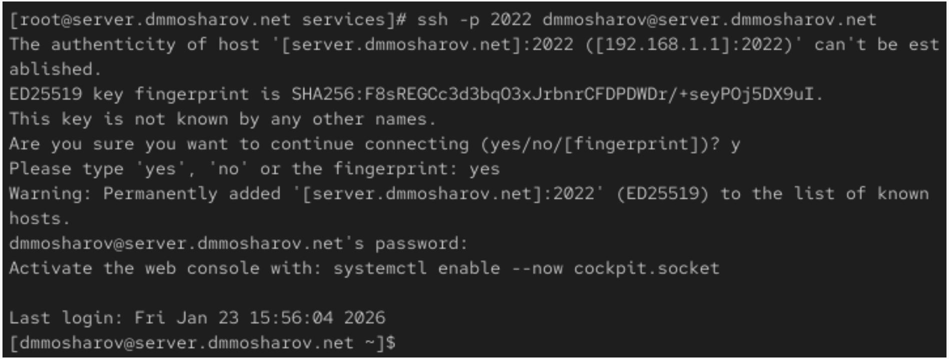
Форвардинг портов



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

Рис. 7: Форвардинг портов

Подключение по ssh

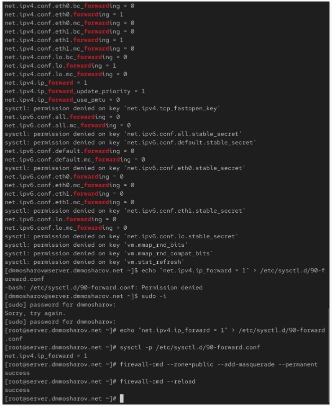


```
[root@server.dmmosharov.net services]# ssh -p 2022 dmmosharov@server.dmmosharov.net
The authenticity of host '[server.dmmosharov.net]:2022 ([192.168.1.1]:2022)' can't be est
ablished.
ED25519 key fingerprint is SHA256:F8sREGCc3d3bqO3xJrbnrCFDPDWDr/+seyPOj5DX9uI.
This key is not known by any other 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 ~]$
```

Рис. 8: Подключение по ssh

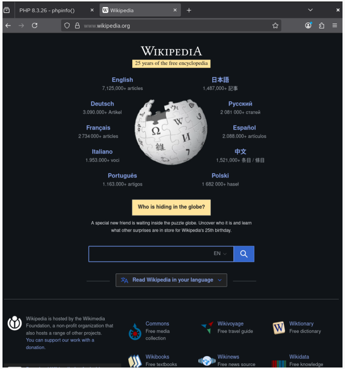
Включение перенаправления и маскарадинга



```
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 ~]# 
```

Рис. 9: Включение перенаправления и маскарадинга

Проверка доступа в интернет



WIKIPEDIA

25 years of the free encyclopedia

English
7,125,000+ articles

日本語
1,487,000+ 記事

Deutsch
3.090.000+ Artikel

Русский
2 081 000+ статей

Français
2 734 000+ articles

Español
2.088.000+ artículos

Italiano
1.953.000+ voci

中文
1,521,000+ 条目 / 條目

Português
1.163.000+ artigos

Polski
1 682 000+ haseł

Who is hiding in the globe?

A special new friend is waiting inside the puzzle globe. Uncover who it is and learn what other surprises are in store for Wikipedia's 25th birthday.

Wikipedia is hosted by the Wikimedia Foundation, a non-profit organization that also hosts a range of other projects. You can support our work with a donation.

Commons
Free media collection

Wikivoyage
Free travel guide

Wiktionary
Free dictionary

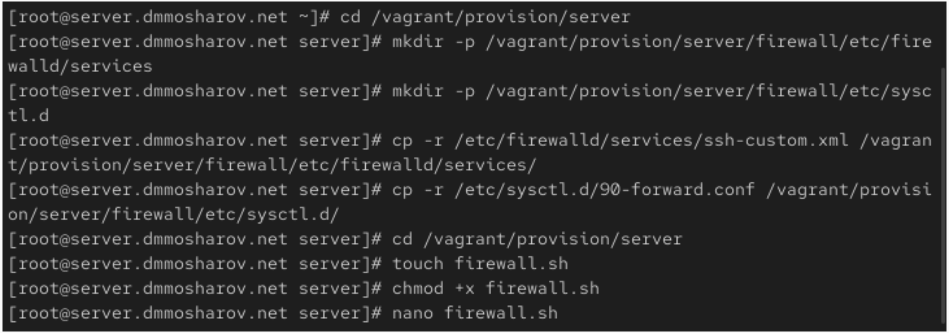
Wikibooks
Free textbooks

Wikinews
Free news source

Wikidata
Free knowledge

Рис. 10: Проверка доступа в интернет

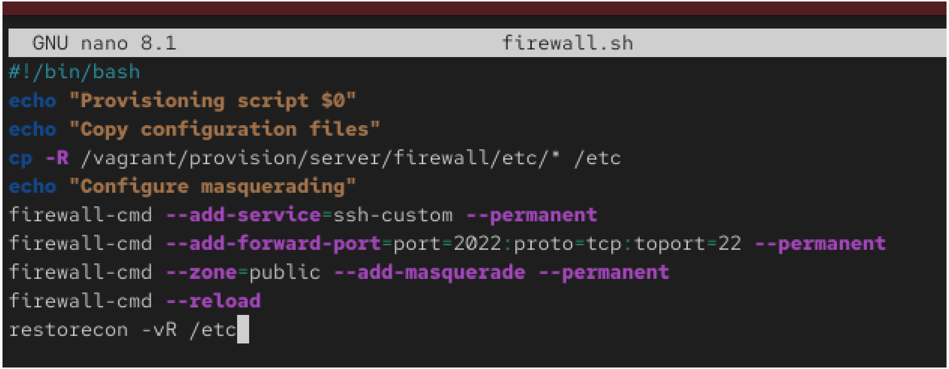
Сохранение конфигурации vagrant



```
[root@server.dmmosharov.net ~]# cd /vagrant/provision/server
[root@server.dmmosharov.net server]# mkdir -p /vagrant/provision/server/firewall/etc/fire
walld/services
[root@server.dmmosharov.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysc
tl.d
[root@server.dmmosharov.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagran
t/provision/server/firewall/etc/firewalld/services/
[root@server.dmmosharov.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provisi
on/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
```

Рис. 11: Сохранение конфигурации vagrant

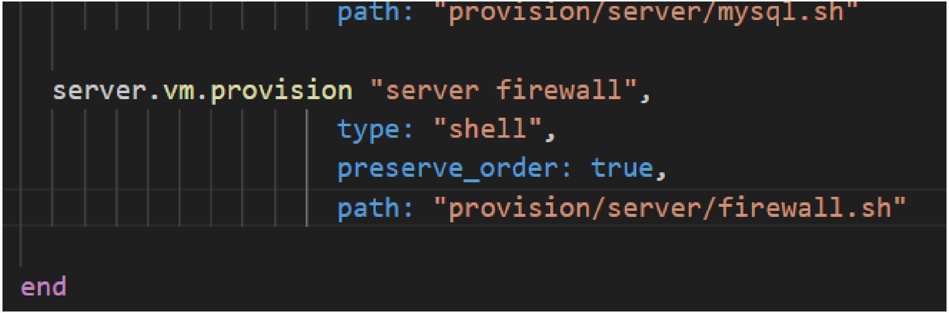
firewall.sh



```
  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
```

Рис. 12: firewall.sh

Vagrantfile



```
                    path: "provision/server/mysql.sh"

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

end
```

Рис. 13: Vagrantfile

Выводы

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