

# Отчет по лабораторной работе №7

Дисциплина:Администрирование сетевых подсистем

Шихалиева Зурият Арсеновна

# Цель работы

Получить навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquearading

# Задание

Настройте межсетевой экран виртуальной машины `server` для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022.

Настройте Port Forwarding на виртуальной машине `server`.

Настройте маскардинг на виртуальной машине `server` для организации доступа клиента к сети Интернет.

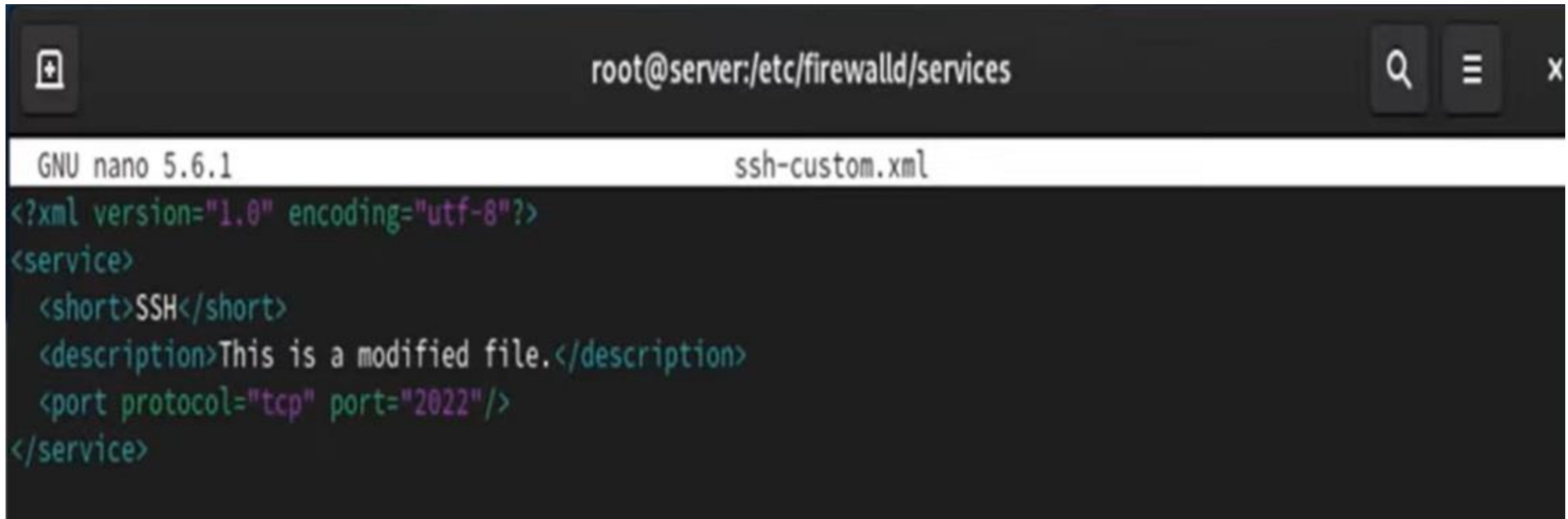
Напишите скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана.

Соответствующим образом внести изменения в Vagrantfile

# Выполнение работы

```
[root@server ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/fire
firefox/ firewallld/
[root@server ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server ~]# cd /etc/firewalld/services/ssh-custom.xml
-bash: cd: /etc/firewalld/services/ssh-custom.xml: Not a directory
[root@server ~]# cd /etc/firewalld/services/
[root@server 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 p
rovides secure encrypted communications. If you plan on accessing your machine remotely via SSH over a firewalle
d interface, enable this option. You need the openssh-server package installed for this option to be useful.</de
scription>
  <port protocol="tcp" port="22"/>
</service>
```

# Выполнение работы



```
root@server:/etc/firewalld/services

GNU nano 5.6.1 ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>This is a modified file.</description>
  <port protocol="tcp" port="2022"/>
</service>
```

# Выполнение работы

```
[root@server 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 ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctddb 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 finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-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
isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-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 kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns
memcache minidlna mongodb mongod ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut
openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus
prometheus-node-exporter proxy-dhcp ps2link ps3netsrv 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 snmptls snmptls-trap snmptrap
spideroak-lansync spotify-sync squid sssd 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 vds 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-agent zabbix-server zerotier
```

# Выполнение работы

- Добавление новой службы и ее активация

```
bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
[root@server services]# firewall-cmd --reload
success
[root@server 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 ceph 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 finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-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 isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-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 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 ntp ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv 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 snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid 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 vds 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-agent zabbix-server zerotier
[root@server services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server services]# firewall-cmd --reload
success
[root@server services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
```

# Выполнение работы

Организуем на сервере переадресацию с порта 2022 на порт 22 с помощью команды:

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



# Выполнение работы

```
[root@server services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
[root@server 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
[root@server services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server services]# firewall-cmd --reload
success
```

# Выполнение работы

- Создание окружения для внесения изменений в настройки окружающей среды

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

# Выполнение работы

A terminal window titled 'root@server:/vagrant/provision/server' with search, menu, and close icons in the top right. The terminal shows the execution of a script named 'firewall.sh' using GNU nano 5.6.1. The script contains several echo statements and firewall commands. The commands executed are: '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', and 'restorecon -vR /etc'.

```
root@server:/vagrant/provision/server
GNU nano 5.6.1 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
```

# Выполнение работы

```
server.vm.network :private_network,  
  ip: "192.168.1.1",  
  virtualbox____intnet: true  
  
server.vm.provision "server dummy",  
  type: "shell",  
  preserve_order: true,  
  path: "provision/server/01-dummy.sh"  
  
server.vm.provision "server dns",  
  type: "shell",  
  preserve_order: true,  
  path: "provision/server/dns.sh"  
  
server.vm.provision "server dhcp",  
  type: "shell",  
  preserve_order: true,  
  path: "provision/server/dhcp.sh"  
  
server.vm.provision "server http",  
  type: "shell",  
  preserve_order: true,  
  path: "provision/server/http.sh"  
  
server.vm.provision "server mysql",  
  type: "shell",  
  preserve_order: true,  
  path: "provision/server/mysql.sh"  
  
server.vm.provision "server firewall",  
  type: "shell",  
  preserve_order: true,  
  path: "provision/server/firewall.sh"
```

# Вывод

В результате выполнения данной работы были приобретены практической настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading