

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ
ПАТРИСА ЛУМУМБЫ**

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

**ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 7**

Дисциплина «Администрирование сетевых подсистем»

Тема «Расширенные настройки межсетевого экрана»

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

МОСКВА

2023 г.

Цель работы

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

Задание

1. Настроить межсетевой экран виртуальной машины server для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022.
2. Настроить Port Forwarding на виртуальной машине server.
3. Настроить маскардинг на виртуальной машине server для организации доступа клиента к сети Интернет.
4. Написать скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внести изменения в Vagrantfile.

Выполнение

1. Создание пользовательской службы firewalld

1. На основе существующего файла описания службы ssh создала файл с собственным описанием и посмотрела содержимое файла службы (рис.1.1).

В файле /etc/firewalld/services/ssh-custom.xml определен пользовательский сервис SSH. Файл представляет собой конфигурацию для firewalld, позволяя настраивать правила файрвола для SSH-сервиса.

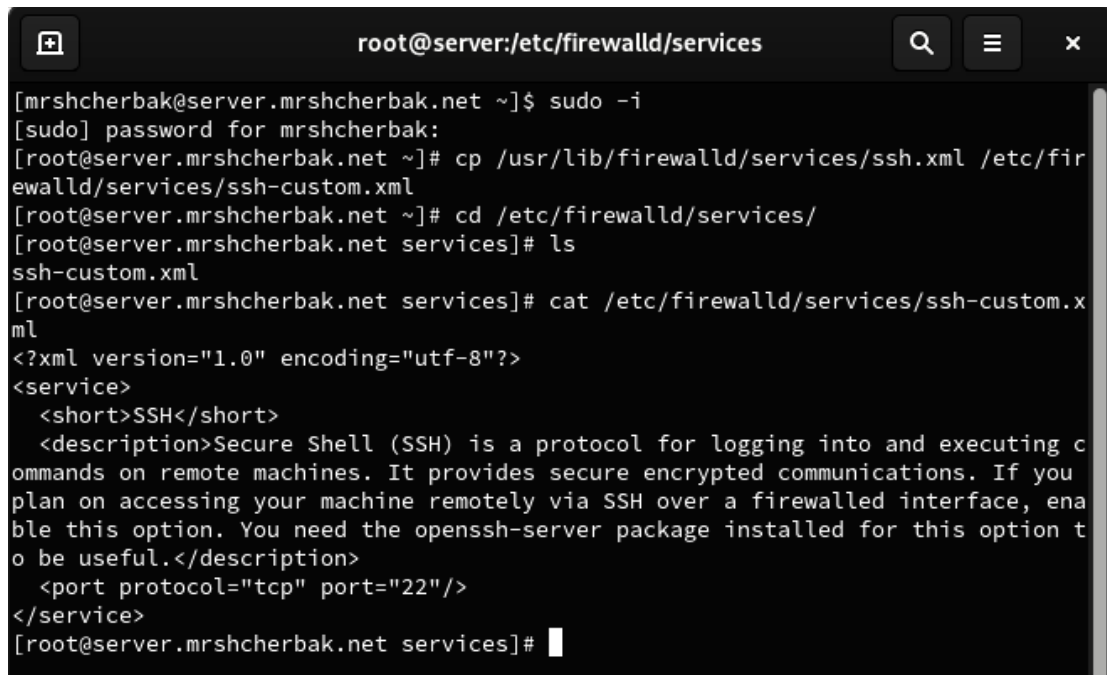
<?xml version="1.0" encoding="utf-8"?>: XML-заголовок, указывающий на версию XML и кодировку символов.

<service>: начало определения сервиса.

<short>SSH</short>: краткое описание сервиса, где указано, что это SSH.

<description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines...: здесь предоставлено более подробное описание сервиса SSH. Объясняется, что SSH - это протокол для входа и выполнения команд на удаленных машинах, обеспечивающий безопасные зашифрованные коммуникации. Также отмечается, что для использования этой опции необходим пакет openssh-server.

<port protocol="tcp" port="22"/>: здесь указывается, что сервис использует TCP-протокол и прослушивает порт 22.

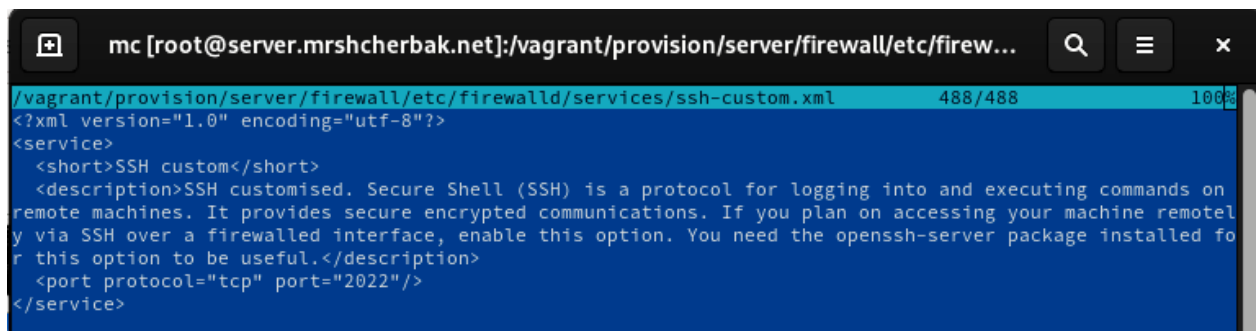


```
root@server:/etc/firewalld/services

[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i
[sudo] password for mrshcherbak:
[root@server.mrshcherbak.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.mrshcherbak.net ~]# cd /etc/firewalld/services/
[root@server.mrshcherbak.net services]# ls
ssh-custom.xml
[root@server.mrshcherbak.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.mrshcherbak.net services]#
```

Рис.1.1. Создание файла ssh-custom.xml и просмотр его содержимого

2. Открыла файл описания службы на редактирование и заменила порт 22 на новый порт (2022), а также скорректировала описание службы для демонстрации, что это модифицированный файл службы (рис.1.2).



```
mc [root@server.mrshcherbak.net]:/vagrant/provision/server/firewall/etc/firew...

/vagrant/provision/server/firewall/etc/firewalld/services/ssh-custom.xml 488/488 100%
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH custom</short>
  <description>SSH customised. 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>
```

Рис.1.2. Редактирование файла ssh-custom.xml

3. Просмотрела список доступных FirewallD служб (рис.1.3). Новая служба ещё не отображается в списке.

```
[root@server.mrshcherbak.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit auswe
isapp2 bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-l
sd ceph ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dhcp dhcpv6 dhcp
v6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-clien
t etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication fre
eipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 h
ttps ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jellyfin jenkins kadmin kdec
onnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-cont
rol-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-sch
eduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt lib
virt-tls lightning-network llmnr llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongod
m mosh mountd mqttd mqttd-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-dashboard nfs nfs3 nmea-0183
nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmw
ebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps3netsrv ptp pulse
audio 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 snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui s
ynergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vds
m vnc-server wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discov
ery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zero
tier
```

Рис.1.3. Просмотр списка доступных FirewallD служб

4. Перегрузила правила межсетевого экрана с сохранением информации о состоянии и вновь вывела на экран список служб, а также список активных служб (рис.1.4). Убедилась, что созданная служба отображается в списке доступных для FirewallD служб, но не активирована.

```
[root@server.mrshcherbak.net services]# firewall-cmd --reload
success
[root@server.mrshcherbak.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit auswe
isapp2 bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-l
sd ceph ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dhcp dhcpv6 dhcp
v6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-clien
t etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication fre
eipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 h
ttps ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jellyfin jenkins kadmin kdec
onnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-cont
rol-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-sch
eduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt lib
virt-tls lightning-network llmnr llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongod
m mosh mountd mqttd mqttd-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-dashboard nfs nfs3 nmea-0183
nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmw
ebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps3netsrv ptp pulse
audio 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 snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn syncthing sync
thing-gui synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp
-client vds m vnc-server wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tc
p ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-
server zerotier
[root@server.mrshcherbak.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.mrshcherbak.net services]#
```

Рис.1.4. Выполнение команд

5. Добавила новую службу в FirewallD и вывела на экран список активных служб (рис.1.5).

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

Рис.1.5. Служба активирована

2. Перенаправление портов

1. Организовала на сервере переадресацию с порта 2022 на порт 22 (рис.2.1).

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

Рис.2.1. Выполнение команды

2. На клиенте попробовала получить доступ по SSH к серверу через порт 2022 (рис.2.2).

```
[root@client.mrshcherbak.net ~]# ssh -p 2022 mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Web console: https://server.mrshcherbak.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Nov 23 21:49:44 2023 from 192.168.1.30
[mrshcherbak@server.mrshcherbak.net ~]$
```

Рис.2.2. Выполнение команды

3. Настройка Port Forwarding и Masquerading

1. На сервере посмотрела, активирована ли в ядре системы возможность перенаправления IPv4-пакетов (рис.3.1).

```
[root@server.mrshcherbak.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
[root@server.mrshcherbak.net services]#
```

Рис.3.1. Возможность перенаправления IPv4-пакетов в ядре системы не активирована

2. Включила перенаправление IPv4-пакетов и маскарадинг на сервере (рис.3.2).

```
[root@server.mrshcherbak.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.mrshcherbak.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.mrshcherbak.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.mrshcherbak.net services]# firewall-cmd --reload
success
```

Рис.3.2. Выполнение команд

3. На клиенте проверила доступность выхода в Интернет (рис.3.3).

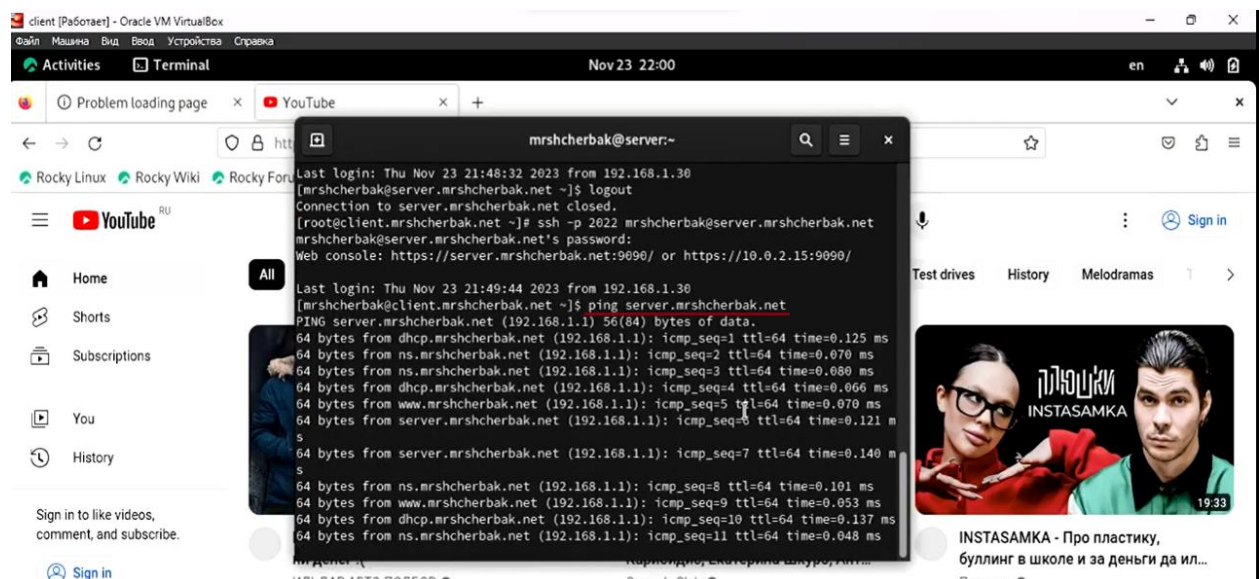


Рис.3.3. Выход в Интернет есть

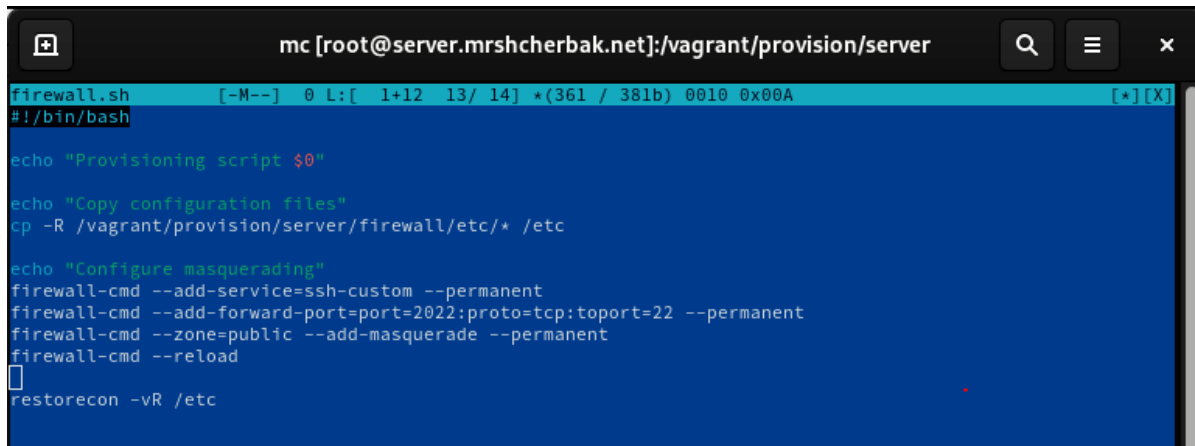
4. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перешла в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создала в нём каталог firewall, в который поместила в соответствующие подкаталоги конфигурационные файлы FirewallD. В каталоге /vagrant/provision/server создала файл firewall.sh. Действия представлены на рис.4.1.

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

Рис.4.1. Выполнение команд

2. Открыв файл firewall.sh на редактирование, прописала в нём скрипт (рис.4.2).



```
mc [root@server.mrshcherbak.net]:/vagrant/provision/server
firewall.sh [-M--] 0 L:[ 1+12 13/ 14] *(361 / 381b) 0010 0x00A [*][X]
#!/bin/bash

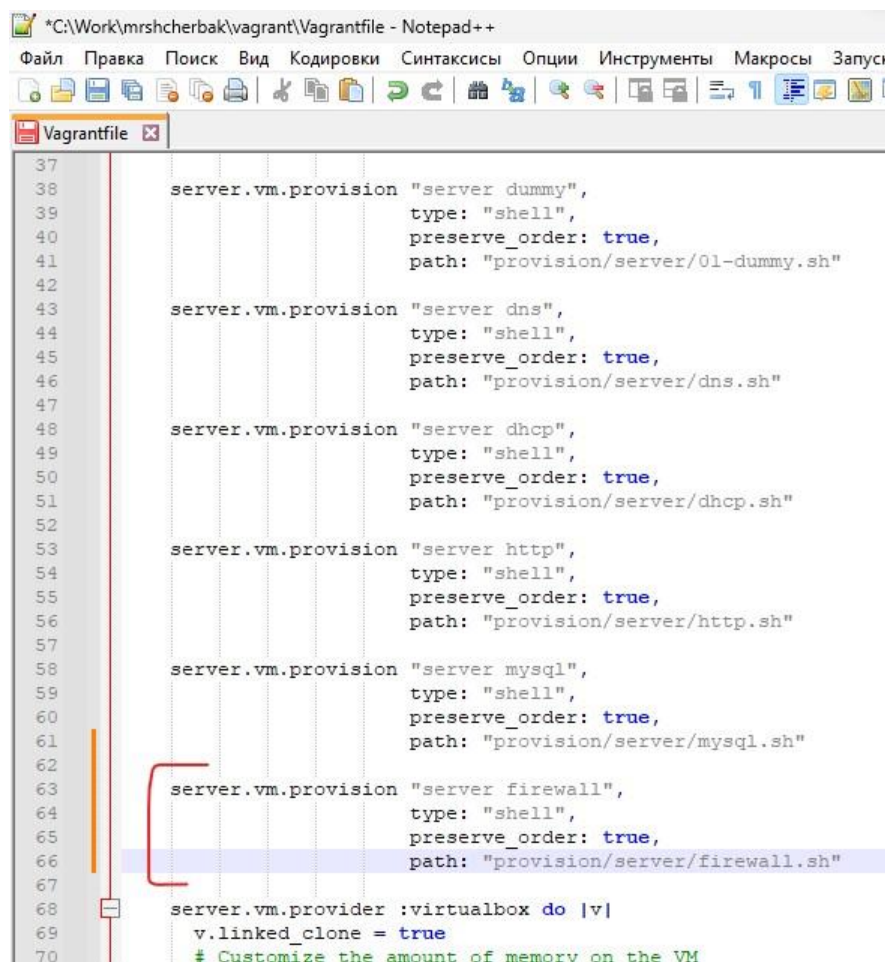
echo "Provisioning script $0"

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.4.2. Редактирование файла firewall.sh

3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавила в разделе конфигурации для сервера запись (рис.4.3).



```
*C:\Work\mrshcherbak\vagrant\Vagrantfile - Notepad++
Файл Правка Поиск Вид Кодировки Синтаксисы Опции Инструменты Макросы Запуск
Vagrantfile
37
38 server.vm.provision "server dummy",
39     type: "shell",
40     preserve_order: true,
41     path: "provision/server/01-dummy.sh"
42
43 server.vm.provision "server dns",
44     type: "shell",
45     preserve_order: true,
46     path: "provision/server/dns.sh"
47
48 server.vm.provision "server dhcp",
49     type: "shell",
50     preserve_order: true,
51     path: "provision/server/dhcp.sh"
52
53 server.vm.provision "server http",
54     type: "shell",
55     preserve_order: true,
56     path: "provision/server/http.sh"
57
58 server.vm.provision "server mysql",
59     type: "shell",
60     preserve_order: true,
61     path: "provision/server/mysql.sh"
62
63 server.vm.provision "server firewall",
64     type: "shell",
65     preserve_order: true,
66     path: "provision/server/firewall.sh"
67
68 server.vm.provider :virtualbox do |v|
69     v.linked_clone = true
70     # Customize the amount of memory on the VM
```

Рис.4.3. Содержимое файла Vagrantfile

Вывод: таким образом, в ходе выполнения л/р №7 я получила навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

Контрольные вопросы

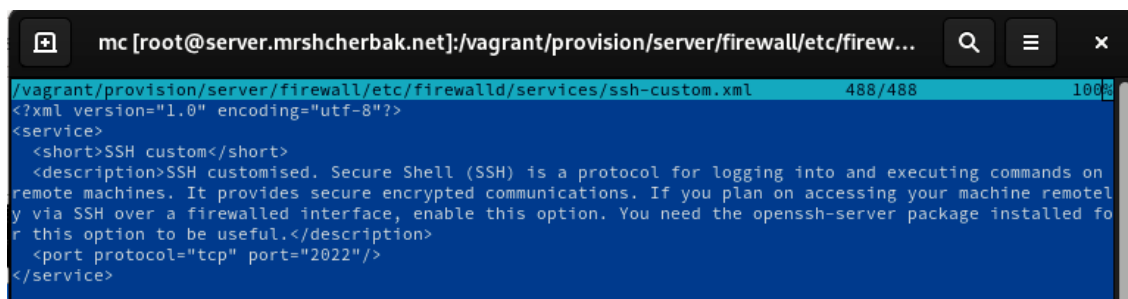
1. Где хранятся пользовательские файлы firewalld?

Пользовательские файлы firewalld обычно хранятся в директории /etc/firewalld/. В данной л/р, например, в файле /etc/firewalld/services/ssh-custom.xml определен пользовательский сервис SSH. Firewalld хранит все настройки, связанные со службами, в XML-файлах в каталоге /usr/lib/firewalld/services. Если требуется переопределить настройки имеющейся службы или подключить собственную службу, то необходимо файл с описанием службы разместить в каталоге /etc/firewalld/services.

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

Для указания порта TCP 2022 в пользовательском файле службы, нужно добавить строку в секцию <port> следующим образом:

<port protocol="tcp" port="2022"/>: здесь указывается, что сервис использует TCP-протокол и прослушивает порт 2022.



```
mc [root@server.mrshcherbak.net]:/vagrant/provision/server/firewall/etc/firew...
/vagrant/provision/server/firewall/etc/firewalld/services/ssh-custom.xml 488/488 100%
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH custom</short>
  <description>SSH customised. 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 remotel
y via SSH over a firewalled interface, enable this option. You need the openssh-server package installed fo
r this option to be useful.</description>
  <port protocol="tcp" port="2022"/>
</service>
```

3. Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере?

Для перечисления всех служб, доступных на сервере, используем команду:

firewall-cmd --get-services

Так, в данной л/р я просматривала список доступных FirewallD служб.


```
[root@server.mrshcherbak.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit auswe
isapp2 bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-l
sd ceph ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dhcp dhcpv6 dhcp
v6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-clien
t etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication fre
eipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 h
ttps ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jellyfin jenkins kadmin kdec
onnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-cont
rol-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-sch
eduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt lib
virt-tls lightning-network llmnr llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb
mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-dashboard nfs nfs3 nmea-0183
nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pncd pmpoxy pmwebapi pmw
ebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps3netsrv ptp pulse
audio 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 snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui s
ynergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vds
m vnc-server wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discov
ery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zero
tier
```

4. В чем разница между трансляцией сетевых адресов (NAT) и маскарadingом (masquerading)?

Разница между NAT и маскарadingом в том, что NAT переводит один IP-адрес в другой, а маскарading скрывает внутренние IP-адреса за единственным внешним IP-адресом. NAT может использовать уникальные или общие внешние адреса, в то время как маскарading всегда использует общий внешний адрес для группы устройств в локальной сети.

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

Команда для разрешения входящего трафика на порт 4404 и перенаправления его на службу SSH по IP-адресу 10.0.0.10 может выглядеть так:

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

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

Для включения маскарadingа IP-пакетов для всех пакетов, выходящих в зону public, используем команду:

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

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