РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 7
Расширенные настройки межсетевого экрана

Дисциплина: Администрирование сетевых подсистем

Студент: Карташова А.С.

Группа: НФИбд-03-18

МОСКВА

2020 г.

Оглавление

Цель работы

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

Задачи

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

2. Настроим Port Forwarding на виртуальной машине server

3. Настроим маскарадинг на виртуальной машине server для организации доступа клиента к сети Интернет

4. Напишем скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внеем изменения в Vagrantfile

Ход работы

Создание пользовательской службы firewalld

На основе существующего файла описания службы ssh создадим файл с собственным описанием и посмотрим содержимое файла службы (ssh-custom.xml)

```
[root@server.askartashova.net services]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-cust
om.xml
[root@server.askartashova.net services]# cd /etc/firewalld/services/
[root@server.askartashova.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 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>
[root@server.askartashova.net services]# nano /etc/firewalld/services/ssh-custom.xml
```

<?xml version="1.0" encoding="utf-8"?> **-** версия докумета и тип шифрования

<service>

<short>SSH</short> **-** краткое назвние службы

<description> description> **-** описание службы

<port protocol="tcp" port="22"/>- номер tcp порта

</service>

Откроем файл описания службы на редактирование и заменим порт 22 на новый порт (2022). Скорректируем описание службы для демонстрации, что это модифицированный файл службы.

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH custom</short>
  <description>ssh-customize</description>
  <port protocol="tcp" port="2022"/>
</service>
```

Просмотрим список доступных FirewallD служб. Новой службы в списке нет.

```
[root@server.askartashova.net services]# firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bacula-client bb bgp bitcoin bitco
in-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit condor-collector ctdb d
hcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd
-client etcd-server finger freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp ganglia-cl
ient ganglia-master git grafana gre high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-
target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-apiserver ldap ldaps libv
irt libvirt-tls lightning-network llmnr managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-
tls ms-wbt mssql murmur mysql nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-v
mconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio
 puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rsh rsyncd rtsp salt-master samba samba-client sa
mba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync spotify-sync squid ssdp ssh
steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tftp-client til
e38 tinc tor-socks transmission-client upnp-client vdsm vnc-server wbem-http wbem-https wsman wsmans xdmcp xmpp-
bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
[root@server.askartashova.net services]#
```

Перегрузим правила межсетевого экрана с сохранением информации о состоянии и вновь выведем на экран список служб и список активных служб.Служба отображается в списке доступных, но она не активна.

```
[root@server.askartashova.net services]# firewall-cmd --reload
success
[root@server.askartashova.net services]# firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bacula-client bb bgp bitcoin bitco
in-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit condor-collector ctdb d
hcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd
-client etcd-server finger freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp ganglia-cl
ient ganglia-master git grafana gre high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-
target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-apiserver ldap ldaps libv
irt libvirt-tls lightning-network llmnr managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-
tls ms-wbt mssql murmur mysql nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-v
mconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio
 puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rsh rsyncd rtsp salt-master samba samba-client sa
mba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync spotify-sync squid ssdp ssh
ssh-custom steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tftp
-client tile38 tinc tor-socks transmission-client upnp-client vdsm vnc-server wbem-http wbem-https wsman wsmans
xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
[root@server.askartashova.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
```

Добавим новую службу в FirewallD и выведем на экран список активных служб

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

Перенаправление портов

Организуем на сервере переадресацию с порта 2022 на порт 22

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

На клиенте попробуем получить доступ по SSH к серверу через порт 2022

```
[root@client.askartashova.net ~]# ssh -p 2022 askartashova@server.askartashova.net
The authenticity of host '[server.askartashova.net]:2022 ([192.168.1.1]:2022)' can't be established.
ECDSA key fingerprint is SHA256:/5/Q+Jtvd/rCSkSnvOX9VjiBd25GqfPJWjr3OY7RCX8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[server.askartashova.net]:2022,[192.168.1.1]:2022' (ECDSA) to the list of
known hosts.
askartashova@server.askartashova.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Dec  4 15:44:01 2020
[askartashova@server.askartashova.net ~]$
```

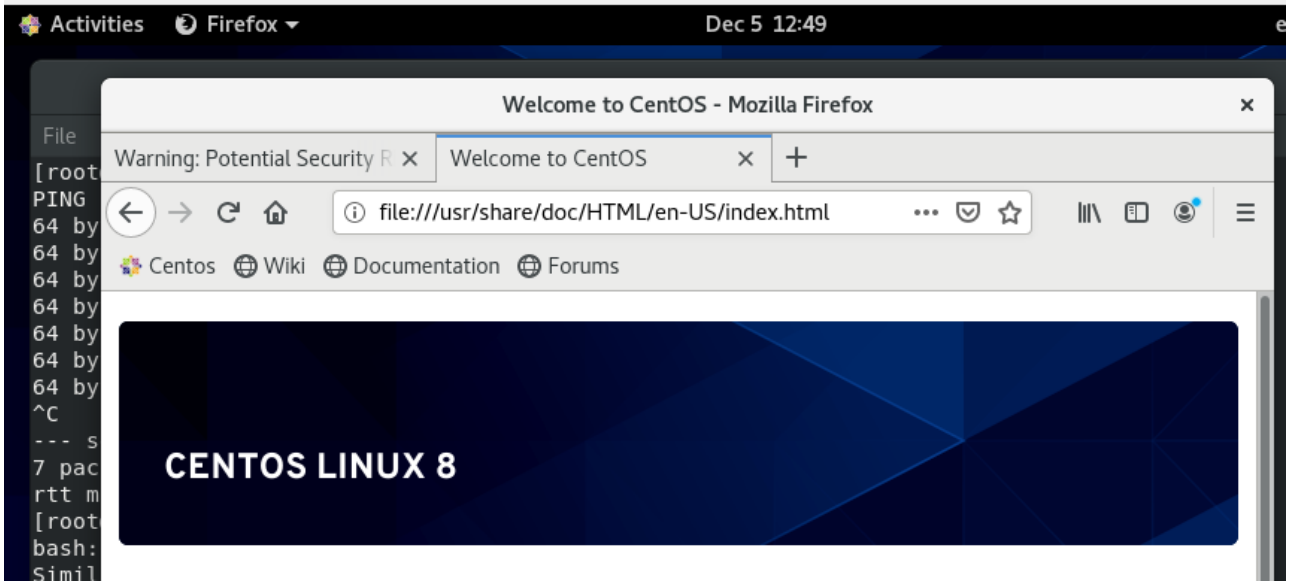
Настройка Port Forwarding и Masquerading

На сервере посмотрим, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов (возможность включена). Включим перенаправление IPv4-пакетов на сервере.

```
rtt min/avg/max/mdev = 0.588/0.652/0.717/0.069 ms
[root@server.askartashova.net named]# sysctl -a | grep forward
net.ipv4.conf.all.bc_forwarding = 0
net.ipv4.conf.all.forwarding = 1
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.default.bc_forwarding = 0
net.ipv4.conf.default.forwarding = 1
net.ipv4.conf.default.mc_forwarding = 0
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.conf.virbr0.bc_forwarding = 0
net.ipv4.conf.virbr0.forwarding = 1
net.ipv4.conf.virbr0.mc_forwarding = 0
net.ipv4.conf.virbr0-nic.bc_forwarding = 0
net.ipv4.conf.virbr0-nic.forwarding = 1
net.ipv4.conf.virbr0-nic.mc_forwarding = 0
net.ipv4.ip_forward = 1
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
```

Включим маскарадинг на сервере и на клиенте проверим, что выход в интернет доступен.

```
[root@server.askartashova.net named]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.askartashova.net named]# sysctl -p rtc/sysctl.d/90-forward.conf
sysctl: cannot open "rtc/sysctl.d/90-forward.conf": No such file or directory
[root@server.askartashova.net named]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.askartashova.net named]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.askartashova.net named]# firewall-cmd --reload
success
```



Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог firewall, в который поместим в соответствующие подкаталоги конфигурационные файлы FirewallD

В каталоге /vagrant/provision/server создадим исполняемый файл firewall.sh, пропишем в нём следующий скрипт, который повторяет произведённые действия по установке и настройке сервера баз данных.

```
[root@server.askartashova.net named]# cd /vagrant/provision/server
[root@server.askartashova.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server.askartashova.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.askartashova.net server]# cp -r /etc/firewalld/services/ssh-custom.xml
cp: missing destination file operand after '/etc/firewalld/services/ssh-custom.xml'
Try 'cp --help' for more information.
[root@server.askartashova.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/serv
rewall/etc/firewalld/services/
[root@server.askartashova.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewa
c/sysctl.d/
[root@server.askartashova.net server]# cd /vagrant/provision/server
[root@server.askartashova.net server]# touch firewall.sh
[root@server.askartashova.net server]# chmod +x firewall.sh
[root@server.askartashova.net server]# nano firewall.sh
```

```
  GNU nano 2.9.8                                          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
```

Для отработки созданного скрипта во время загрузки виртуальных машин в конфигурационном файле Vagrantfile добавим в конфигурации сервера следующую запись:

server.vm.provision "server firewall",
type: "shell",

preserve_order: true,

path: "provision/server/firewall.sh"

```
# Server configuration

config.vm.define "server", autostart: false do |server|
  server.vm.box = "centos8"
  server.vm.hostname = 'server'

  server.ssh.insert_key = false
  server.ssh.username = 'vagrant'
  server.ssh.password = 'vagrant'

  server.vm.network :private_network, ip: "192.168.1.1", virtualbox__intnet: true

 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 dummy",
    type: "shell",
    preserve_order: true,
    path: "provision/server/01-dummy.sh"

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

Заключение

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

Контрольные вопросы

1.Где хранятся пользовательские файлы firewalld?

Описания хранятся в:

/usr/lib/firewalld/services/

Пользовательские файлы хранятся в

/etc/firewalld/services/

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

<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 маскарадингом (masquerading)?

(NAT) — механизм преобразования IP-адресов транзитных пакетов. Может производить замену алреса на любой указанный.

Маскарадинг (Masquerading) — тип трансляции сетевого адреса, при которой вместо адреса отправителя динамически подставляется адрес назначенного интерфейса. Использует NAT для замены обратного сетевого адреса пакетов на сетевой адресс шлюза.

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=ssh:toaddr=10.0.0.10

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

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