РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 7

дисциплина: Администрирование сетевых подсистем

Студент: Бакулин Никита 1032201747

Группа: НПИбд-01-20

МОСКВА

2022 г.

Постановка задачи

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

Выполнение работы

1.

1.1. На основе существующего файла описания службы ssh создайте файл с собственным описанием

1.2. Посмотрите содержимое файла службы

1.3. Откройте файл описания службы на редактирование и замените порт 22 на новый порт (2022)

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>[EDITED] Secure Shell (SSH) is a protocol for logging into and ex
ecuting commands on remote machines. It provides secure encrypted communications
. If you plan on accessing your machine remotely via SSH over a firewalled inter
face, enable this option. You need the openssh-server package installed for this
 option to be useful.</description>
  <port protocol="tcp" port="2022"/>
</service>
```

Рисунок 1

1.4. Просмотрите список доступных FirewallD служб: firewall-cmd --get-services Обратите внимание, что новая служба ещё не отображается в списке

1.5. Перегрузите правила межсетевого экрана с сохранением информации о состоянии и вновь выведите на экран список служб, а также список активных служб

1.6. Добавьте новую службу в FirewallD и выведите на экран список активных служб

```
[nabakulin@server.nabakulin.net ~]$ sudo -i
[sudo] password for nabakulin:
[root@server.nabakulin.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.nabakulin.net ~]# cd /etc/firewalld/services/
[root@server.nabakulin.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 communicatio
ns. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the openssh-server package insta
lled for this option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server.nabakulin.net services]# vi /etc/firewalld/services/ssh-custom.xml
[root@server.nabakulin.net services]# vi /etc/firewalld/services/ssh-custom.xml
[root@server.nabakulin.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin
-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd condor-collector ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-ov
er-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 grafana gre high-availability http https imap imaps ipp ipp-cli
ent ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane
 kube-controller-manager kube-scheduler kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr managesieve matrix mdns memcache minidl
na mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storagecons
ole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio puppetmaster quassel radi
us 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 snm
p snmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle
tftp tile38 tinc tor-socks transmission-client upnp-client vdsm vnc-server wbem-http wbem-https wireguard wsman wsmans xdmcp xmpp-bosh xmpp-client xm
pp-local xmpp-server zabbix-agent zabbix-server
[root@server.nabakulin.net services]# firewall-cmd --reload
success
[root@server.nabakulin.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin
-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd condor-collector ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-ov
er-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 grafana gre high-availability http https imap imaps ipp ipp-cli
ent ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane
 kube-controller-manager kube-scheduler kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr managesieve matrix mdns memcache minidl
na mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storagecons
ole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio puppetmaster quassel radi
us 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 snm
p snmptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telne
t tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsm vnc-server wbem-http wbem-https wireguard wsman wsmans xdmcp xmpp-bosh xmp
p-client xmpp-local xmpp-server zabbix-agent zabbix-server
[root@server.nabakulin.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.nabakulin.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.nabakulin.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
```

Рисунок 2

2.

2.1. Организуйте на сервере переадресацию с порта 2022 на порт 22

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

Рисунок 3

2.2. На клиенте попробуйте получить доступ по SSH к серверу через порт 2022

```
[nabakulin@client.nabakulin.net ~]$ ssh -p 2022 nabakulin@server.nabakulin.net
The authenticity of host '[server.nabakulin.net]:2022 ([192.168.1.1]:2022)' can'
t be established.
ED25519 key fingerprint is SHA256:zqbOam9bCTBqb0qNzuP7z0xlgOqvGhkHxMkw2sQdblo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[server.nabakulin.net]:2022' (ED25519) to the list o
f known hosts.
nabakulin@server.nabakulin.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Dec  4 03:01:10 2022
[nabakulin@server.nabakulin.net ~]$
```

Рисунок 4

3.

3.1. На сервере посмотрите, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов

3.2. Включите перенаправление IPv4-пакетов на сервере

3.3. Включите маскарадинг на сервере

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

Рисунок 5

3.4. На клиенте проверьте доступность выхода в Интернет

```
[nabakulin@client.nabakulin.net ~]$ ping ya.ru
PING ya.ru (87.250.250.242) 56(84) bytes of data.
64 bytes from ya.ru (87.250.250.242): icmp_seq=1 ttl=244 time=14.7 ms
64 bytes from ya.ru (87.250.250.242): icmp_seq=2 ttl=244 time=14.0 ms
64 bytes from ya.ru (87.250.250.242): icmp_seq=3 ttl=244 time=13.9 ms
64 bytes from ya.ru (87.250.250.242): icmp_seq=4 ttl=244 time=14.8 ms
64 bytes from ya.ru (87.250.250.242): icmp_seq=5 ttl=244 time=14.3 ms
^C
--- ya.ru ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 10835ms
rtt min/avg/max/mdev = 13.916/14.347/14.806/0.355 ms
```

Рисунок 6

4.

4.1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог firewall, в который поместите в соответствующие подкаталоги конфигурационные файлы FirewallD

4.2. В каталоге /vagrant/provision/server создайте файл 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
```

Рисунок 7

4.3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера

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

Рисунок 8

Контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?
   /usr/lib/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)?
   Маскардинг - замена адреса на адрес машины, выполняющей маскарад, а NAT - замена адреса на любой указанный

5. Какая команда используется для включения маскарадинга IP-пакетов для всех

пакетов, выходящих в зону public?

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