

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: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

МОСКВА

2022 г.

Цель работы:

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

Выполнение работы:

1. Создание пользовательской службы firewallld

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

```
cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
cd /etc/firewalld/services/
```

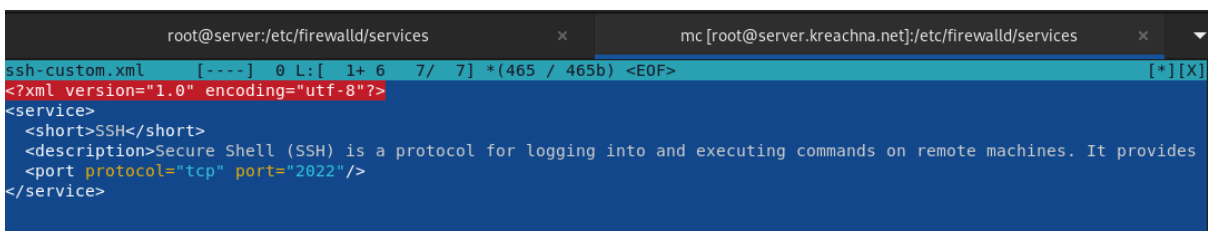
```
[kreachna@server.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@server.kreachna.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.kreachna.net ~]# cd /etc/firewalld/services/
```

2. Посмотрите содержимое файла службы:

```
cat /etc/firewalld/services/ssh-custom.xml
```

```
[root@server.kreachna.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>
```

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



```
root@server:/etc/firewalld/services  x  mc [root@server.kreachna.net]:/etc/firewalld/services  x  ▾
ssh-custom.xml  [---]  0 L:[ 1+ 6 7/ 7] *(465 / 465b) <EOF>  [*][X]
<?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
  <port protocol="tcp" port="2022"/>
</service>
```

4. Просмотрите список доступных FirewallD служб:

```
firewall-cmd --get-services
```

```
[root@server.kreachna.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-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 grafana gre high-availability http https imap imaps
ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibanalogin
kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-controller-manager kube-scheduler
kubenetd kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr managesieve matrix
mdns memcached minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns
nfs nfs3 nmap nmap-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole
plex pncd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp 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 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
vdsms vnc-server wbem-http wbem-https wireguard wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local
xmpp-server zabbix-agent zabbix-server
```

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

```
firewall-cmd --reload
firewall-cmd --get-services
firewall-cmd --list-services
```

```
[root@server.kreachna.net services]# firewall-cmd --reload
success
[root@server.kreachna.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-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 grafana gre high-availability http https imap imaps
ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibanalogin
kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-controller-manager kube-scheduler
kubenetd kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr managesieve matrix
mdns memcached minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns
nfs nfs3 nmap nmap-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole
plex pncd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp 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 snmptrap
spideroak-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui
synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client
vdsms vnc-server wbem-http wbem-https wireguard wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local
xmpp-server zabbix-agent zabbix-server
[root@server.kreachna.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
```

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

```
firewall-cmd --add-service=ssh-custom
firewall-cmd --list-services
```

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

2. Перенаправление портов

1. Организуйте на сервере переадресацию с порта 2022 на порт 22:

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

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

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

```
ssh -p 2022 kreachna@server.kreachna.net
```

```
[kreachna@client.kreachna.net ~]$ ssh -p 2022 kreachna@server.kreachna.net
The authenticity of host '[server.kreachna.net]:2022 ([192.168.1.1]:2022)' can't
be established.
ED25519 key fingerprint is SHA256:/2uvDHfM1QlaLTeqPJTnsRSAYzizIaAix/x7vXlm2m4.
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.kreachna.net]:2022' (ED25519) to the list of
known hosts.
kreachna@server.kreachna.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Thu Dec  1 18:59:54 2022
```

3. Настройка Port Forwarding и Masquerading

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

```
sysctl -a | grep forward
```

```
[root@server.kreachna.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
```

2. Включите перенаправление IPv4-пакетов на сервере:

```
echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
sysctl -p /etc/sysctl.d/90-forward.conf
```

```
[root@server.kreachna.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.kreachna.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
```

3. Включите маскардинг на сервере:

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

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

4. На клиенте проверьте доступность выхода в Интернет.

```
[kreachna@server.kreachna.net ~]$ ping www.yandex.ru
PING www.yandex.ru (5.255.255.70) 56(84) bytes of data.
64 bytes from 5.255.255.70 (5.255.255.70): icmp_seq=1 ttl=52 time=10.3 ms
64 bytes from 5.255.255.70 (5.255.255.70): icmp_seq=2 ttl=52 time=10.5 ms
64 bytes from yandex.ru (5.255.255.70): icmp_seq=3 ttl=52 time=15.4 ms
64 bytes from yandex.ru (5.255.255.70): icmp_seq=4 ttl=52 time=10.5 ms
64 bytes from yandex.ru (5.255.255.70): icmp_seq=5 ttl=52 time=9.92 ms
64 bytes from yandex.ru (5.255.255.70): icmp_seq=6 ttl=52 time=9.22 ms
^C
--- www.yandex.ru ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5802ms
rtt min/avg/max/mdev = 9.224/10.981/15.449/2.045 ms
```

4. Внесение изменений в настройки внутреннего окружения виртуальной машины

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:

```
[root@server.kreachna.net services]# cd /vagrant/provision/server
[root@server.kreachna.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server.kreachna.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.kreachna.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/se
rver/firewall/etc/firewalld/services/
[root@server.kreachna.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/fire
wall/etc/sysctl.d/
```

2. В каталоге /vagrant/provision/server создайте файл firewall.sh:

```
[root@server.kreachna.net server]# cd /vagrant/provision/server
[root@server.kreachna.net server]# touch firewall.sh
[root@server.kreachna.net server]# chmod +x firewall.sh
[root@server.kreachna.net server]# vim firewall.sh
```

Открыв его на редактирование, пропишите в нём следующий скрипт:

```
root@server:/vagrant/provision/server x mc [root@server.k
#!/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
~
```

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

```
Vagrantfile x
52     preserve_order: true,
53     path: "provision/server/http.sh"
54
55     server.vm.provision "server mysql",
56     type: "shell",
57     preserve_order: true,
58     path: "provision/server/mysql.sh"
59
60     server.vm.provision "server firewall",
61     type: "shell",
62     preserve_order: true,
63     path: "provision/server/firewall.sh"
64
```

Ответ на контрольные вопрос

1. Где хранятся пользовательские файлы firewalld?
/usr/lib/firewalld/services/ssh.xml
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 маскарadingом (masquerading)?
NAT производит замену адреса на любой указанный, а маскарading только на адрес, машины, выполняющей маскаррад.

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 маскардинга IP-пакетов для всех пакетов, выходящих в зону public?

```
firewall-cmd --zone=public --add-masquerad
```

Вывод:

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