

Лабораторная работа №7

Расширенные настройки межсетевого экрана

Беличева Дарья Михайловна

Российский университет дружбы народов, Москва, Россия

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

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 маскарading 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 лабораторной работы

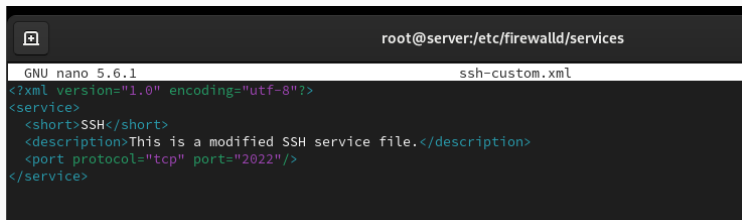
Создание пользовательской службы firewalld

На основе существующего файла описания службы ssh создадим файл с собственным описанием и посмотрим содержимое файла службы.

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

Рис. 1: Создание файла с собственным описанием

Создание пользовательской службы firewalld



```
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 SSH service file.</description>
  <port protocol="tcp" port="2022"/>
</service>
```

Рис. 2: Отредактированный файл описания службы

Создание пользовательской службы firewallld

Просмотрим список доступных FirewallD служб. Новая служба ещё не отображается в списке.

```
[root@server.dmbelicheva.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacu
la-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine checkmk-ag
ent cockpit collectd condor-collector cratedb ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry dock
er-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeip
a-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 jellyfin jenkins kadmin kdeconnec
t kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-c
ontroller-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-tcp llmnr-udp manage
sieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-da
shboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwe
bapi pmwebapis pop3 pop3s postgresql proxo proxyd prometheus prometheus-node-exporter proxy-dhcp ps3netshr ptp pulseaudio pupp
etmaster 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 ssd
p ssh steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-so
cks transmission-client upnp-client vds vnc-server wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-di
scovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server z
erotier
```

Рис. 3: Список доступных FirewallD служб

Создание пользовательской службы firewalld

```
[root@server.dmbelicheva.net services]# firewall-cmd --reload
success
[root@server.dmbelicheva.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacu
la-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine checkmk-ag
ent cockpit collectd condor-collector cratedb ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry dock
er-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeip
a-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 jellyfin jenkins kadmin kdeconnec
t kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-c
ontroller-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-tcp llmnr-udp manage
sieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-da
shboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwe
bapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps3netsrv ptp pulseaudio pupp
etmaster 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 ssd
p ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tile38
tinc tor-socks transmission-client unpn-client vdsman vnc-server wbem-http wbem-https wireguard ws-discovery ws-discovery-c
lient ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbbx-agent zabb
ix-server zerotier
[root@server.dmbelicheva.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.dmbelicheva.net services]# firewall-cmd --add-service-ssh-custom
success
[root@server.dmbelicheva.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.dmbelicheva.net services]#
```

Рис. 4: Список Firewalld служб и добавление новой службы в Firewalld

Организуем на сервере переадресацию с порта 2022 на порт 22. На клиенте попробуем получить доступ по SSH к серверу через порт 2022:

```
[root@server.dmbelicheva.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
[root@server.dmbelicheva.net services]# ssh -p 2022 dmbelicheva@server.dmbelicheva.net
ssh: connect to host server.dmbelicheva.net port 2022: Connection refused
```

Рис. 5: Переадресация и получение доступа по SSH

Настройка Port Forwarding и Masquerading

```
[root@server.dmbelicheva.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
```

Рис. 6: Проверка активации перенаправления IPv4-пакетов

Настройка Port Forwarding и Masquerading

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

Рис. 7: Включение перенаправление IPv4-пакетов и маскардинга на сервере

Настройка Port Forwarding и Masquerading

На клиенте проверим доступность выхода в Интернет.

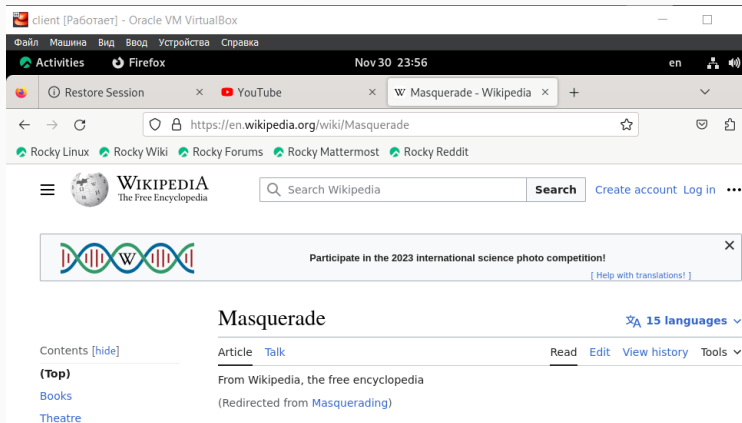


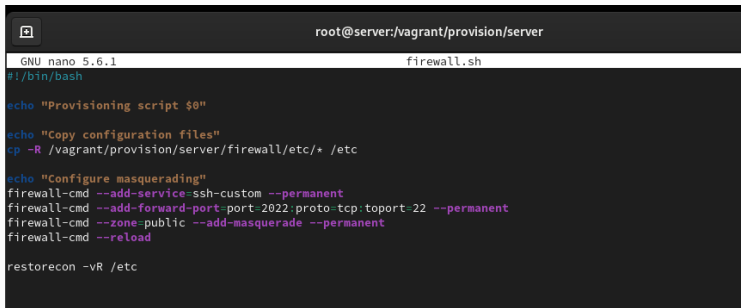
Рис. 8: Проверка доступности выхода в Интернет

Внесение изменений в настройки внутреннего окружения виртуальной машины

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

Рис. 9: Внесения изменений в настройки внутреннего окружения

Внесение изменений в настройки внутреннего окружения виртуальной машины



```
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
```

Рис. 10: Редактирование файла

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"
```

В процессе выполнения данной лабораторной работы я получила навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.