

Лабораторная работа № 7.

Расширенные настройки межсетевого экрана

Студент: Яссин оулед салеи

НПИбд-02-20

Цель работы

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


Задание

- 1. Настройте межсетевой экран виртуальной машины server для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022 (см. разделы 7.4.1 и 7.4.2).
- 2. Настройте Port Forwarding на виртуальной машине server (см. разделы 7.4.3).
- 3. Настройте маскерадинг на виртуальной машине server для организации доступа клиента к сети Интернет (см. раздел 7.4.3).
- 4. Напишите скрипт для Vagrant, фиксирующий действия по расширенной настройке меж сетевого экрана. Соответствующим образом внести изменения в Vagrantfile (см. раздел 7.4.4).

Создание пользовательской службы firewalld

```
root@server:/etc/firewalld/services  x  root@server:~  x  v
<?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="2022"/>
</service>
~
~
~
~
~

[root@server.yassine.net services]# firewall-cmd --reload
success
[root@server.yassine.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 ceph-fengine 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-tar get 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 minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns nfs nfs3 nmap-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquodad 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 sssd 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 vds vnc-server wbem-http wbem-https wireguard wsmannet xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
[root@server.yassine.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.yassine.net services]#
```



. Настройка Port Forwarding и Masquerading

```
cockpit dhcp dnsv6-client dns http https ssh ssh-custom
[root@server.yassine.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
Warning: ALREADY_ENABLED: '2022:tcp:22:' already in 'public'
success
[root@server.yassine.net services]#
```

```
[yassine@client.yassine.net ~]$ ssh -p 2022 yassine@server.yassine.net
The authenticity of host '[server.yassine.net]:2022 ([192.168.1.1]:2022)' can't
be established.
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0qNzuP7z0xlg0qvGhkHxMkw2sQdblo.
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.yassine.net]:2022' (ED25519) to the list of
known hosts.
yassine@server.yassine.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Nov 28 10:41:25 2022
[yassine@server.yassine.net ~]$
```

Настройка Port Forwarding и Masquerading

```
[root@server.yassine.net ~]# systemctl -a | grep forward
net.ipv4.conf.all.bc_forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.nc_forwarding = 0
net.ipv4.conf.default.bc_forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.nc_forwarding = 0
net.ipv4.conf.eth0.bc_forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.nc_forwarding = 0
net.ipv4.conf.eth1.bc_forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.nc_forwarding = 0
net.ipv4.conf.lo.bc_forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.nc_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_ptu = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.all.nc_forwarding = 0
```

```
[yassine@client.yassine.net ~]$ ssh -p 2022 yassine@server.yassine.net
The authenticity of host '[server.yassine.net]:2022 ([192.168.1.1]:2022)' can't
be established.
ED25519 key fingerprint is SHA256:zqb0am9bCTBqB0qNzuP7z0xlq0vGhkHxMkw2sQdblo.
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.yassine.net]:2022' (ED25519) to the list of
known hosts.
yassine@server.yassine.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Nov 28 10:41:25 2022
[yassine@server.yassine.net ~]$
```

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

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

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
root@server:/vagrant/provision/server

/bin/bash

cho "Provision script $0"

cho "Copy configuration files"
cp -R /vagrant/provision/server/firewall/etc/* /etc

cho "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

storecon -vR /etc
```

```
root@server.yassine.net ~]# cd /vagrant/provision/server
root@server.yassine.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
root@server.yassine.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
root@server.yassine.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/
firewall/etc/firewalld/services/
cp: missing destination file operand after '/etc/firewalld/services/ssh-custom.xml/vagrant/provision/server/
firewall/etc/firewalld/services/'
Try 'cp --help' for more information.
root@server.yassine.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/
firewall/etc/firewalld/services/
root@server.yassine.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/
etc/sysctl.d/
root@server.yassine.net server]#
```

ВЫВОД

- Получил навыки настройки межсетевого экрана в Linux в части переедресации портов и настройки Masquerading.