

Лабораторная работа №7

Расширенные настройки межсетевого экрана

Демидова Е. А.

19 ноября 2023

Российский университет дружбы народов, Москва, Россия

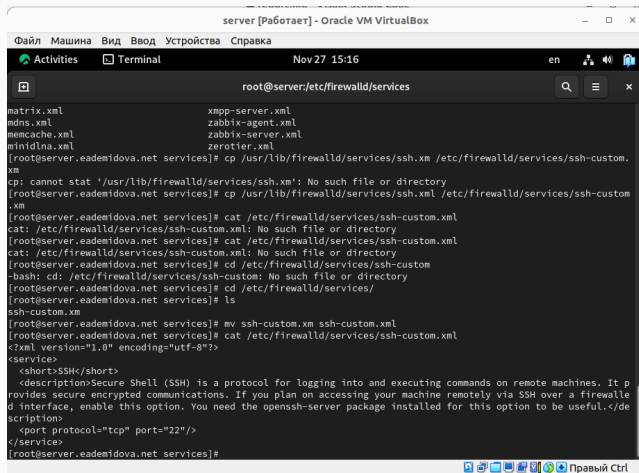
Вводная часть

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

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 маскарading 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 лабораторной работы

Создание пользовательской службы firewalld

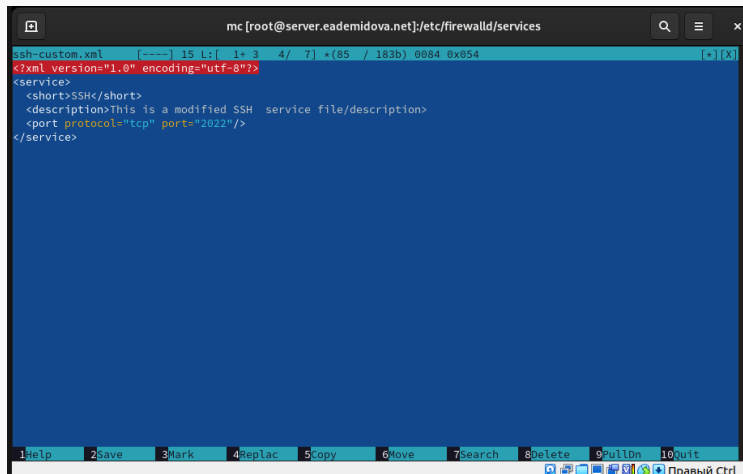


```
server [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Activities  Terminal  Nov 27 15:16  en  [audio icon]  [network icon]
root@server:/etc/firewalld/services

matrix.xml          xmpp-server.xml
mdns.xml            zabbix-agent.xml
memcache.xml        zabbix-server.xml
minidlna.xml        zerotier.xml
[root@server.eademidova.net services]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
cp: cannot stat '/usr/lib/firewalld/services/ssh.xml': No such file or directory
[root@server.eademidova.net services]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
cat: /etc/firewalld/services/ssh-custom.xml: No such file or directory
[root@server.eademidova.net services]# cat /etc/firewalld/services/ssh-custom.xml
cat: /etc/firewalld/services/ssh-custom.xml: No such file or directory
[root@server.eademidova.net services]# cd /etc/firewalld/services/ssh-custom
-bash: cd: /etc/firewalld/services/ssh-custom: No such file or directory
[root@server.eademidova.net services]# cd /etc/firewalld/services/
[root@server.eademidova.net services]# ls
ssh-custom.xml
[root@server.eademidova.net services]# mv ssh-custom.xml ssh-custom.xml
[root@server.eademidova.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 firewall d 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.eademidova.net services]#
```

Рис. 1: Содержание файла службы ssh

Создание пользовательской службы firewallld



The screenshot shows a text editor window titled "mc [root@server.eademidova.net]:/etc/firewalld/services". The editor is displaying the content of a file named "ssh-custom.xml". The text is as follows:

```
ssh-custom.xml  [----] 15 L:[ 1+ 3 4/ 7] *(85 / 183b) 0084 0x054 [ * ] [ X ]
<?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>
```

At the bottom of the editor, there is a toolbar with the following items: 1Help, 2Save, 3Mark, 4Replac, 5Copy, 6Move, 7Search, 8Delete, 9PullDn, 10Quit. Below the toolbar, there are icons for various functions and the text "Правый Ctrl".

Рис. 2: Редактирование файла службы SSH

Создание пользовательской службы firewalld

```

root@server:/etc/firewalld/services

<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 firewall 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.eademidova.net services]# mc

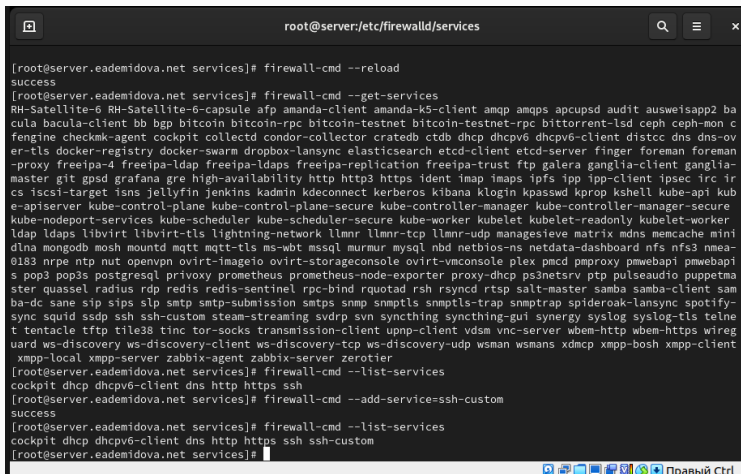
[root@server.eademidova.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon ceph-fengine checkmk-agent cockpit collectd condor-collector cratedb 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-ltd freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jellyfin jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-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 managesieve matrix mdns memcache mini-dlna mongod mosh moshm mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-dashboards nfs nfs3 nmap-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapi-s pop3 pop3s postgresql proxy prometheus prometheus-node-exporter proxy-dhcp ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rsh rsyncd rtsp salt-master samba samba-client samba-ba-dc sane sip sipd smtp smtp-submission smtps snmp snmpd1 snmpd1s snmpd1s-trap 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 vdsman vnc-server wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier

[root@server.eademidova.net services]#

```

Рис. 3: Список доступным FirewallD служб

Создание пользовательской службы firewalld



```
root@server:/etc/firewalld/services

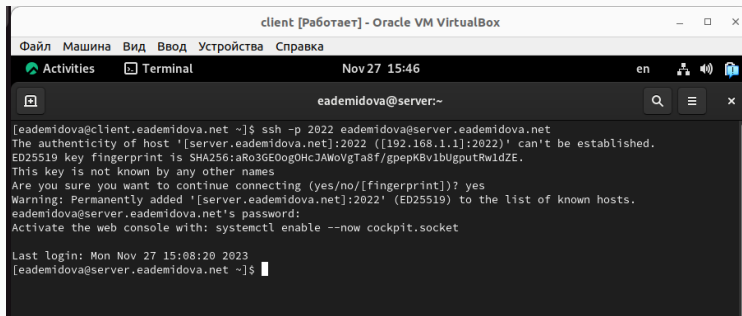
[root@server.eademidova.net services]# firewall-cmd --reload
success
[root@server.eademidova.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 ba
cula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon c
fengine checkmk-agent cockpit collectd condor-collector cratedb 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 gpsd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ir
cs iscsi-target isns jellyfin jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kub
e-apiserver kube-control-plane kube-control-plane-secure kube-controller-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 managesieve matrix mdns memcache mini
dlna mongodb mosh mounstd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-dashboard nfs nfs3 nmea-
0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapi
s pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps3netshv ptp pulseaudio puppetma
ster quassel radius rdp redis redis-sentinel rpc-bind rquotat rsh rsyncd rtsp salt-master samba samba-client sam
ba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-
sync squid sssd 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 vdsms vnc-server wbem-http wbem-https wireg
uard ws-discovery ws-discovery-client ws-discovery-client ws-discovery-udp wsmans wsmans xdmcp xmpp-bosh xmpp-client
xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
[root@server.eademidova.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.eademidova.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.eademidova.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.eademidova.net services]#
```

Рис. 4: Добавление новой службы и её активация

Организуем на сервере переадресацию с порта 2022 на порт 22 с помощью команды:

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

Перенаправление портов



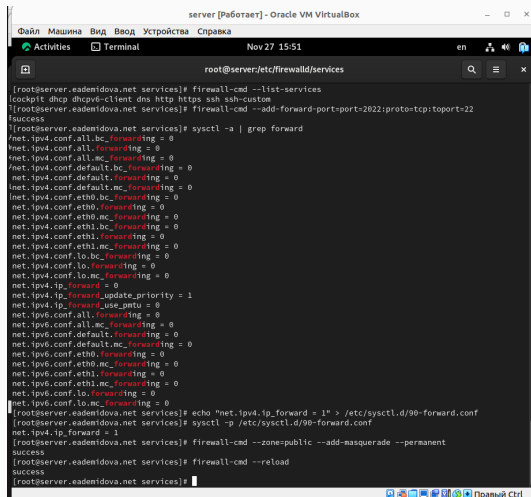
The screenshot shows a terminal window titled "client [Работает] - Oracle VM VirtualBox". The terminal interface includes a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu is a status bar with "Activities", "Terminal", and the date/time "Nov 27 15:46". The terminal prompt is "eademidova@server:~". The user has executed the command `ssh -p 2022 eademidova@server.eademidova.net`. The output shows a warning about the host's authenticity, a fingerprint, and a confirmation to add the host to the known hosts list. The user has accepted the warning, and the terminal shows the prompt "eademidova@server.eademidova.net's password:" followed by a prompt to activate the web console. The terminal also shows the last login time and the current prompt.

```
client [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Activities  Terminal  Nov 27 15:46  en  [icons]
eademidova@server:~
[eademidova@client.eademidova.net ~]$ ssh -p 2022 eademidova@server.eademidova.net
The authenticity of host '[server.eademidova.net]:2022 ([192.168.1.1]:2022)' can't be established.
ED25519 key fingerprint is SHA256:aRo3GE0og0HcJAWoVgTa8f/gpepKBv1bUgputRwldZE.
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.eademidova.net]:2022' (ED25519) to the list of known hosts.
eademidova@server.eademidova.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Nov 27 15:08:20 2023
[eademidova@server.eademidova.net ~]$
```

Рис. 5: Получение клиентом удаленного доступа по SSH к серверу через порт 2022

Настройка Port Forwarding и Masquerading



```
server [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Activities Terminal Nov27 15:51
root@server:/etc/firewalld/services

[root@server.eadmidova.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.eadmidova.net services]# firewall-cmd --add-forward-port=port:2022:proto=tcp:toport=22
success
[root@server.eadmidova.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.eadmidova.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.eadmidova.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.eadmidova.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.eadmidova.net services]# firewall-cmd --reload
success
[root@server.eadmidova.net services]#
```

Рис. 6: Настройка перенаправления IPv4-пакетов и включение маскардинга

Внесение изменений в настройки внутреннего окружения виртуальной машины

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


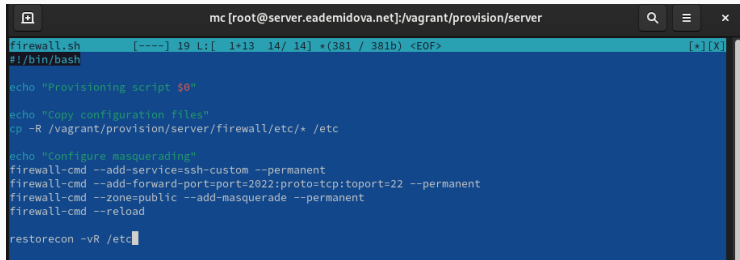


Рис. 7: Создание окружения для внесения изменений в настройки окружающей среды

Внесение изменений в настройки внутреннего окружения виртуальной машины



```
mc [root@server.eademidova.net]:/vagrant/provision/server
firewall.sh [-----] 19 L: [ 1+13 14/ 14] *(381 / 381b) <EOF> [*][X]
#!/bin/bash

echo "Provisioning script $0"

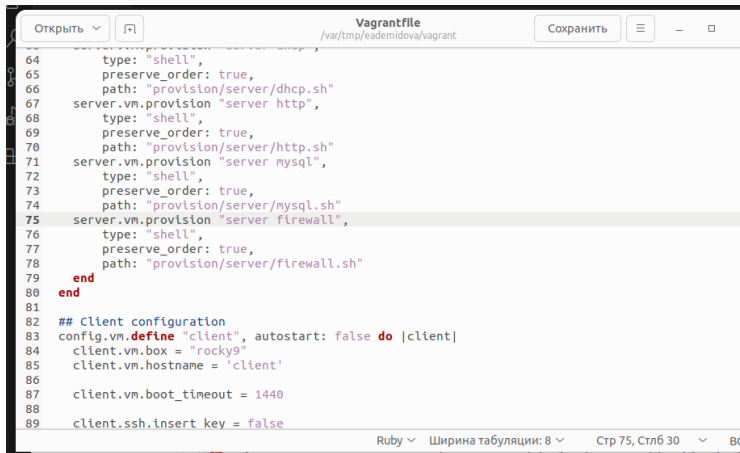
echo "Copy configuration files"
cp -R /vagrant/provision/server/firewall/etc/* /etc

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. 8: Содержание firewall.sh

Внесение изменений в настройки внутреннего окружения виртуальной машины



The image shows a code editor window titled "Vagrantfile" with the path "/var/tmp/eademidova/vagrant". The editor contains a Vagrantfile script. Line 75, which defines the "server firewall" provision, is highlighted. The script includes provisions for shell, http, and mysql services, followed by a firewall provision. Below these, there is a section for client configuration.

```
64     type: "shell",
65     preserve_order: true,
66     path: "provision/server/dhcp.sh"
67   server.vm.provision "server http",
68     type: "shell",
69     preserve_order: true,
70     path: "provision/server/http.sh"
71   server.vm.provision "server mysql",
72     type: "shell",
73     preserve_order: true,
74     path: "provision/server/mysql.sh"
75   server.vm.provision "server firewall",
76     type: "shell",
77     preserve_order: true,
78     path: "provision/server/firewall.sh"
79   end
80 end
81
82 ## Client configuration
83 config.vm.define "client", autostart: false do |client|
84   client.vm.box = "rocky9"
85   client.vm.hostname = 'client'
86
87   client.vm.boot_timeout = 1440
88
89   client.ssh.insert key = false
```

Рис. 9: Изменение файла Vagrantfile

Заключение

В результате выполнения данной работы были приобретены практические навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.