

Отчёт по лабораторной работе 7

Расширенные настройки межсетевого экрана

Метвалли Ахмед Фарг Набеев

Содержание

1	Цель работы	5
2	Выполнение	6
2.1	Создание пользовательской службы firewalld	6
3	Выполнение	10
3.1	Перенаправление портов	10
3.2	Настройка Port Forwarding и Masquerading	11
3.3	Внесение изменений во внутренние настройки виртуальной машины	13
4	Заключение	14
5	Контрольные вопросы	15

Список иллюстраций

2.1	Создание файла ssh-custom.xml и просмотр содержимого	6
2.2	Редактирование файла ssh-custom.xml	7
2.3	Список служб firewalld до перезагрузки	8
2.4	Служба ssh-custom после перезагрузки firewalld	8
2.5	Добавление и активация пользовательской службы	9
3.1	Подключение к серверу по порту 2022	10
3.2	Проверка параметра ip_forward	11
3.3	Включение пересылки IPv4-пакетов	12
3.4	Проверка доступа в Интернет с клиента	12
3.5	Создание структуры каталогов и скрипта firewall.sh	13

Список таблиц

1 Цель работы

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

2 Выполнение

2.1 Создание пользовательской службы firewalld

1. На виртуальной машине server создана пользовательская служба для **firewalld**, основанная на стандартной службе ssh.
2. На основе системного файла `/usr/lib/firewalld/services/ssh.xml` был создан новый файл **ssh-custom.xml** в каталоге `/etc/firewalld/services/`.

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

Рис. 2.1: Создание файла ssh-custom.xml и просмотр содержимого

3. В исходном файле заданы основные элементы XML-описания службы:
 - `<?xml version="1.0" encoding="utf-8"?>` — объявление версии и кодировки XML;
 - `<service>` — корневой элемент, описывающий сетевую службу;

- `<short>` — краткое имя службы, отображаемое в списках `firewalld`;
- `<description>` — текстовое описание назначения службы и её особенностей;
- `<port protocol="tcp" port="22"/>` — определение используемого сетевого порта и протокола.

После редактирования порт был изменён с **22** на **2022**, а в описании указано, что это модифицированная служба.

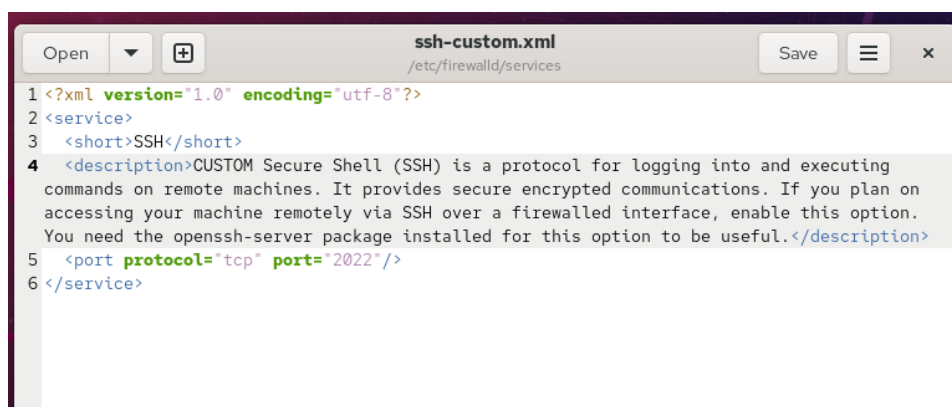


Рис. 2.2: Редактирование файла `ssh-custom.xml`

4. Для проверки доступных служб `firewalld` выполнена команда:

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

В списке отображаются все предустановленные службы, однако созданная служба `ssh-custom` на этом этапе ещё отсутствует.

```
[root@server.ahmedfarg.net services]#
[root@server.ahmedfarg.net services]# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800
apcpsd aseqnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bit
coin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-a
gent civilization-iv civilization-v cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast d
hcp dhcpv6 dhcpv6-client distcc dns dns-over-quick dns-over-tls docker-registry docker-swarm dropbox-lansync elasti
csearch etcd-client etcd-server factorio 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 ht
tp3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdec
nnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-se
cure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-s
ecure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr l
lmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd m
qtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3
nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy
pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv
ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp
salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submissio
n smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfe
r steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing syncthing-g
ui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmi
ssion-client turn turns upnp-client vdsms vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws
-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsd wsd-http wsmn wsmans xdmcp xmpp-bosh
xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-servic
e zero-k zerotier
[root@server.ahmedfarg.net services]#
```

Рис. 2.3: Список служб firewalld до перезагрузки

5. После перезагрузки конфигурации firewalld командами:

```
firewall-cmd --reload
```

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

служба ssh-custom появилась в списке доступных.

```
[root@server.ahmedfarg.net services]#
[root@server.ahmedfarg.net services]# firewall-cmd --reload
success
[root@server.ahmedfarg.net services]# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800
apcpsd aseqnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bit
coin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-a
gent civilization-iv civilization-v cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast d
hcp dhcpv6 dhcpv6-client distcc dns dns-over-quick dns-over-tls docker-registry docker-swarm dropbox-lansync elasti
csearch etcd-client etcd-server factorio 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 ht
tp3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdec
nnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-se
cure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-s
ecure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr l
lmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd m
qtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3
nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy
pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv
ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp
salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submissio
n smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom statsrv steam-
lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing
syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-so
cks transmission-client turn turns upnp-client vdsms vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-d
iscovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsd wsd-http wsmn wsmans xdmcp
xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix
-web-service zero-k zerotier
[root@server.ahmedfarg.net services]#
```

Рис. 2.4: Служба ssh-custom после перезагрузки firewalld

6. Далее выполнено добавление пользовательской службы в список активных:


```
firewall-cmd --add-service=ssh-custom
firewall-cmd --add-service=ssh-custom --permanent
firewall-cmd --reload
```

После этого служба **ssh-custom** успешно активирована и отображается в списке активных служб.

```
[root@server.ahmedfarg.net ~]#
[root@server.ahmedfarg.net services]#
[root@server.ahmedfarg.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.ahmedfarg.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.ahmedfarg.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.ahmedfarg.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.ahmedfarg.net services]# firewall-cmd --reload
success
[root@server.ahmedfarg.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
[root@server.ahmedfarg.net services]# █
```

Рис. 2.5: Добавление и активация пользовательской службы

3 Выполнение

3.1 Перенаправление портов

1. На сервере выполнена настройка переадресации входящих подключений с порта **2022** на порт **22** с помощью команды:

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

2. На клиентской машине выполнено подключение к серверу по SSH через порт **2022**.

Подключение прошло успешно, что подтверждает корректную работу правила переадресации.



```
ahmedfarg@server:~ -- ssh -p 2022 ahmedfarg@server.ahmedf...  
[ahmedfarg@client.ahmedfarg.net ~]$ ssh -p 2022 ahmedfarg@server.ahmedfarg.net  
The authenticity of host '[server.ahmedfarg.net]:2022 ([192.168.1.1]:2022)' can't  
be established.  
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.  
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.ahmedfarg.net]:2022' (ED25519) to the list o  
f known hosts.  
ahmedfarg@server.ahmedfarg.net's password:  
Web console: https://server.ahmedfarg.net:9090/ or https://192.168.1.1:9090/  
  
Last login: Thu Oct  2 08:17:56 2025  
[ahmedfarg@server.ahmedfarg.net ~]$  
[ahmedfarg@server.ahmedfarg.net ~]$
```

Рис. 3.1: Подключение к серверу по порту 2022

3.2 Настройка Port Forwarding и Masquerading

1. На сервере проверено текущее состояние параметра перенаправления IPv4-пакетов.

По выводу команды видно, что параметр `net.ipv4.ip_forward` установлен в значение `0`, то есть переадресация отключена.

```
[root@server.ahmedfarg.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.ahmedfarg.net services]#
```

Рис. 3.2: Проверка параметра `ip_forward`

2. Для включения пересылки IPv4-пакетов создан файл `/etc/sysctl.d/90-forward.conf` с содержимым `net.ipv4.ip_forward = 1`.

После применения параметров командой `sysctl -p /etc/sysctl.d/90-forward.conf` пересылка пакетов успешно активировалась.

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

Рис. 3.3: Включение пересылки IPv4-пакетов

3. Включён маскарадинг в зоне **public** для обеспечения NAT и маршрутизации.

После перезагрузки конфигурации (`firewall-cmd --reload`) система подтвердила успешное применение настроек.

4. С клиентской машины выполнена проверка выхода в Интернет — соединение установлено успешно, что подтверждает корректность настроек перенаправления и маскарадинга.

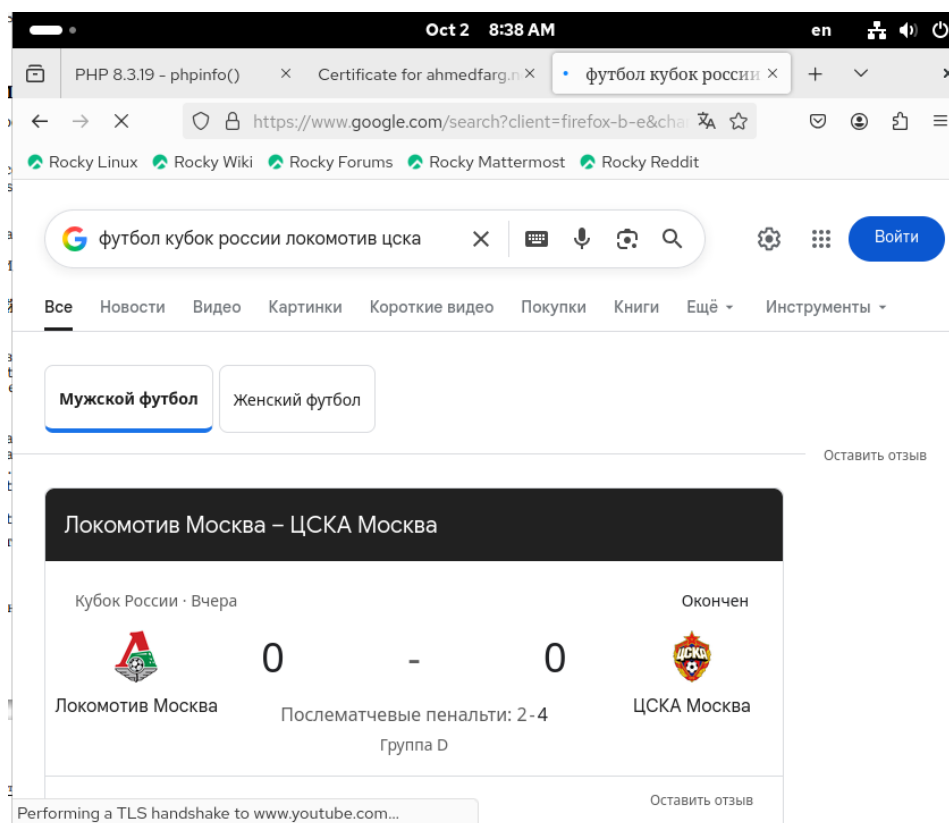


Рис. 3.4: Проверка доступа в Интернет с клиента

3.3 Внесение изменений во внутренние настройки виртуальной машины

1. На сервере создана структура каталогов для хранения конфигурационных файлов **Firewalld** и системных параметров:

- /vagrant/provision/server/firewall/etc/firewalld/services
- /vagrant/provision/server/firewall/etc/sysctl.d

В соответствующие каталоги скопированы файлы `ssh-custom.xml` и `90-forward.conf`.

2. Затем в каталоге /vagrant/provision/server/ создан исполняемый файл **firewall.sh**, предназначенный для автоматического применения конфигурации при разворачивании виртуальной машины.

A terminal window showing a series of commands to create a directory structure and copy files for firewall configuration. The commands are: 1. cd /vagrant/provision/server/ 2. mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services 3. mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d 4. cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/services/ 5. cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d/ 6. touch firewall.sh. The prompt is [root@server.ahmedfarg.net server]#.

```
[root@server.ahmedfarg.net services]#  
[root@server.ahmedfarg.net services]# cd /vagrant/provision/server/  
[root@server.ahmedfarg.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services  
[root@server.ahmedfarg.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d  
[root@server.ahmedfarg.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewal  
l/etc/firewalld/services/  
[root@server.ahmedfarg.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sys  
ctl.d/  
[root@server.ahmedfarg.net server]# touch firewall.sh  
[root@server.ahmedfarg.net server]#
```

Рис. 3.5: Создание структуры каталогов и скрипта `firewall.sh`

4 Заключение

Была выполнена настройка пользовательской службы **firewalld** с переназначением порта SSH на 2022.

Проверена возможность подключения по новому порту, реализовано перенаправление и включён маскрадинг.

Создана структура каталогов и подготовлены конфигурационные файлы для автоматического применения параметров при развёртывании виртуальной машины.

5 Контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?

В каталоге `/etc/firewalld/services/`, где можно размещать собственные XML-файлы описания служб.

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 — общий механизм подмены адресов при прохождении пакетов через маршрутизатор.

Маскарадинг — частный случай NAT, при котором исходящий трафик получает динамический внешний IP-адрес интерфейса, через который осуществляется доступ в сеть.

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=tcp:toaddr=10.0.0.10:toport=22
```

6. Какая команда используется для включения маскарadingа IP-пакетов

для всех пакетов, выходящих в зону public?

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