

# **Лабораторная работа № 13**

**Отчёт**

Ермишина Мария Кирилловна

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение лабораторной работы</b>	<b>6</b>
<b>3 Контрольные вопросы</b>	<b>12</b>
<b>4 Выводы</b>	<b>13</b>

# **Список иллюстраций**

2.1 Добавление конфигураций . . . . .	8
2.2 Настройки брандмауэра . . . . .	9
2.3 Управление брандмауэром с помощью firewall-config . . . . .	10
2.4 Самостоятельная работа . . . . .	11

# **Список таблиц**

# **1 Цель работы**

Целью данной лабораторной работы является получение навыков настройки пакетного фильтра в Linux.

## **2 Выполнение лабораторной работы**

1. Управление брандмауэром с помощью firewall-cmd  
Запустите терминал и получите полномочия администратора. Определите текущую зону по умолчанию, введя: (рис. ??)
  - `firewall-cmd --get-default-zone` Определите доступные зоны, введя: (рис. ??)
  - `firewall-cmd --get-zones` Посмотрите службы, доступные на вашем компьютере, используя (рис. ??)
  - `firewall-cmd --get-services` Определите доступные службы в текущей зоне: (рис. ??)
  - `firewall-cmd --list-services` Сравните результаты вывода информации при использовании команд: (рис. ??)
  - `firewall-cmd --list-all`
  - `firewall-cmd --list-all --zone=public` (рис. ??) Добавьте сервер VNC в конфигурацию брандмауэра: (рис. ??)
  - `firewall-cmd --add-service=vnc-server` Проверьте, добавился ли vnc-server в конфигурацию: (рис. ??)
  - `firewall-cmd --list-all` Перезапустите службу firewalld: (рис. ??)
  - `systemctl restart firewalld` Проверьте, есть ли vnc-server в конфигурации: (рис. ??)
  - `firewall-cmd --list-all`

```
(ermimash@ermimash ~]$ su -
Password:
[root@ermimash ~]# firewall-cmd --get-default-zone
public
[root@ermimash ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@ermimash ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afa amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula
acula-client baros-director baros-filedaemon baros-storage bb bcp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-test
et-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ct
b dds dds-multicast dds-unicast dhcpc dhcpcv6 dhcpcv6-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 free
ipa-replication freeipa-trust freeipa-ganglia-client ganglia-master git gosu grafana gre high-availability http htt
p https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target ismn jenkins kadmin kdeconnect kerberos kib
a klogon kpsswmp kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-ma
nager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet k
ubelet-readonly kubeblet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-tcp llmnr-udp
manageservice matrix mdns memcache minidlna mongod mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbb
os-ns netdata-dashboard nfs nfss nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovir
t-vmconsole plex pmproxy pmwebapi pmwebapis pop3 postgresql privoxy prometheus prometheus-node-exporter prox
y-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rootd rpc-bind rquotad r
h rsysnd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps smpp smptls smpt
s-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui synct
hing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsm v
c-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-uds
wsman wsman-xmpp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
[root@ermimash ~]# firewall-cmd --list-services
cockpit dhcpcv6-client ssh
[root@ermimash ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
[root@ermimash ~]# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  rich rules:
[root@ermimash ~]# firewall-cmd --add-service=vnc-server
success
[root@ermimash ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  rich rules:
[root@ermimash ~]# systemctl restart firewalld
[root@ermimash ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
```

Добавьте службу vnc-server ещё раз, но на этот раз сделайте её постоянной, используя команду (рис. 2.1) - `firewall-cmd --add-service=vnc-server --permanent` Проверьте наличие vnc-server в конфигурации: (рис. 2.1) - `firewall-cmd --list-all` Перезагрузите конфигурацию firewalld и просмотрите конфигурацию времени выполнения: (рис. 2.1) - `firewall-cmd --reload` - `firewall-cmd --list-all` Добавьте в конфигурацию межсетевого экрана порт 2022 протокола TCP: (рис. 2.1) - `firewall-cmd --add-port=2022/tcp --permanent` Затем перезагрузите конфигурацию firewalld: (рис. 2.1) - `firewall-cmd --reload` Проверьте, что порт добавлен в конфигурацию: (рис. 2.1) - `firewall-cmd --list-all`

```
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
    forward: yes
    masquerade: no
    forward-ports:
    source-ports:
    icmp-blocks:
    rich rules:
[root@terminash ~]# firewall-cmd --reload
success
[root@terminash ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh vnc-server
  ports:
  protocols:
    forward: yes
    masquerade: no
    forward-ports:
    source-ports:
    icmp-blocks:
    rich rules:
[root@terminash ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@terminash ~]# firewall-cmd --reload
success
[root@terminash ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
    forward: yes
    masquerade: no
    forward-ports:
    source-ports:
```

Рис. 2.1: Добавление конфигураций

2. Управление брандмауэром с помощью `firewall-config` Откройте терминал и под учётной записью своего пользователя запустите интерфейс GUI `firewall-config`: (рис. 2.3)
  - `firewall-config`

Нажмите выпадающее меню рядом с параметром Configuration (рис. 2.2) Откройте раскрывающийся список и выберите Permanent. Это позволит сделать постоянными все изменения, которые вы вносите при конфигурировании Выберите зону public и отметьте службы http, https и ftp, чтобы включить их. Выберите вкладку Ports и на этой вкладке нажмите Add . Введите порт 2022 и протокол udp, нажмите OK , чтобы добавить их в список. Закройте утилиту `firewall-config`

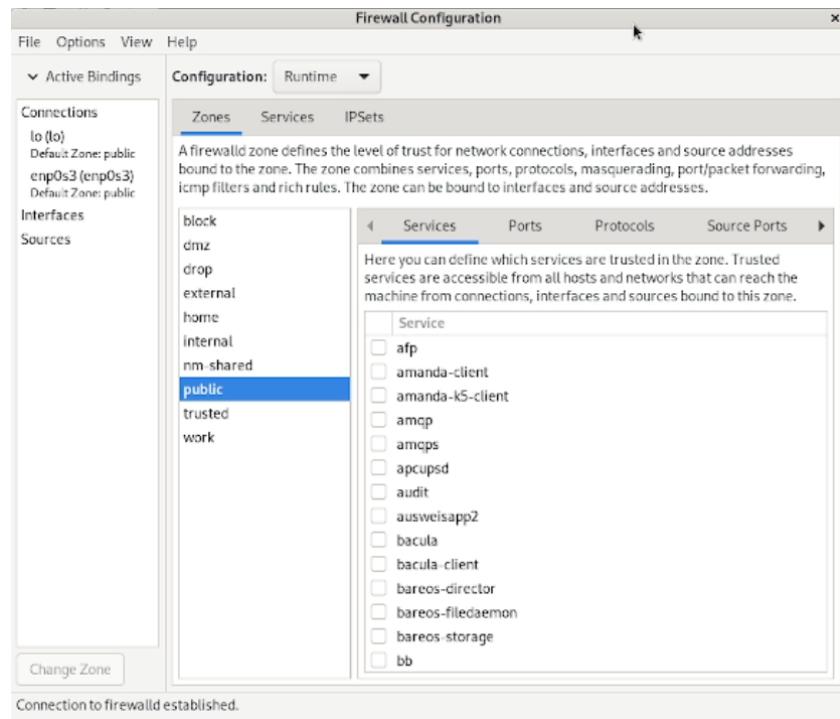


Рис. 2.2: Настройки брандмауэра

В окне терминала введите (рис. 2.3) - `firewall-cmd –list-all` Перегрузите конфигурацию `firewall-cmd`: (рис. 2.3) - `firewall-cmd –reload` и список доступных сервисов:

- `firewall-cmd –list-all`

```

* Waiting in queue...
* Loading list of packages...
The following packages have to be installed:
dbus-x11-1:1.12.20-8.el9.x86_64           X11-requiring add-ons for D-BUS
firewall-config-1.3.4-15.el9_6.noarch        Firewall configuration application
Proceed with changes? [N/y] y

* Waiting in queue...
* Waiting for authentication...

* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...

[ermimash@ermimash ~]$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[ermimash@ermimash ~]$ firewall-cmd --reload
success
[ermimash@ermimash ~]$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ftp http https ssh vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

```

Рис. 2.3: Управление брандмауэром с помощью firewall-config

3. Самостоятельная работа (рис. 2.4) Создайте конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам:

- telnet;
- imap;
- pop3;
- smtp. Сделайте это как в командной строке (для службы telnet), так и в графическом интерфейсе (для служб imap, pop3, smtp) Убедитесь, что конфигурация является постоянной и будет активирована после перезагрузки компьютера

```
[ermimash@ermimash ~]$ firewall-cmd --reload
success
[ermimash@ermimash ~]$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ftp http https ssh vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[ermimash@ermimash ~]$ su -
Password:
[root@ermimash ~]# firewall-cmd --add-service=telnet --permanent
success
[root@ermimash ~]# firewall-config
[root@ermimash ~]# firewall-cmd --reload
success
[root@ermimash ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ftp http https imap[redacted]3 smtp ssh telnet vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
```

Рис. 2.4: Самостоятельная работа

### **3 Контрольные вопросы**

1. sudo systemctl start firewalld
2. firewall-cmd -add-port/udp –permanent
3. firewall-cmd –list-all-zones
4. firewall-cmd –remove-service=vnc-server
5. firewall-cmd –reload
6. firewall-cmd –list-all –zone=
7. firewall-cmd –zone=public –change-interface=en0
8. В зону по умолчанию (firewall-cmd –get-default-zone)

## **4 Выводы**

Получены навыки настройки пакетного фильтра в Linux.