

# **Лабораторная работа № 13. Фильтр пакетов**

**Дисциплина: Основы администрирования операционных систем**

Жукова Арина Александровна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>7</b>
3.1	Управление брандмауэром с помощью firewall-cmd . . . . .	7
3.2	Управление брандмауэром с помощью firewall-config . . . . .	11
3.3	Самостоятельная работа . . . . .	13
<b>4</b>	<b>Выводы</b>	<b>15</b>
	<b>Список литературы</b>	<b>16</b>

# Список иллюстраций

3.1	Определение текущей зоны по умолчанию, доступной зоны, доступные службы на компьютере, доступные зоны в текущей зоне . . . .	7
3.2	Результаты вывода двух команд . . . . .	8
3.3	Добавление VNC сервера . . . . .	8
3.4	Перезапуск службы, проверка наличия сервера . . . . .	9
3.5	Добавление постоянной службы vnc-server . . . . .	9
3.6	Перезагрузка конфигурации . . . . .	10
3.7	Добавление межсетевого экрана, перезагрузка конфигурации . . .	10
3.8	Интерфейс GUI firewall-config . . . . .	11
3.9	Добавление нового порта . . . . .	12
3.10	Проверка подключения серверов . . . . .	13
3.11	Добавление службы telnet . . . . .	13
3.12	Добавление через графический интерфейс . . . . .	14
3.13	Проверка добавления . . . . .	14

## **Список таблиц**

# 1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

## 2 Задание

1. Используя `firewall-cmd`: – определить текущую зону по умолчанию; – определить доступные для настройки зоны; – определить службы, включённые в текущую зону; – добавить сервер VNC в конфигурацию брандмауэра.
2. Используя `firewall-config`: – добавьте службы `http` и `ssh` в зону `public`; – добавьте порт 2022 протокола UDP в зону `public`; – добавьте службу `ftp`.
3. Выполните задание для самостоятельной работы (раздел 13.5).

## 3 Выполнение лабораторной работы

### 3.1 Управление брандмауэром с помощью firewall-cmd

1. Определила текущую зону по умолчанию, используя `firewall-cmd --get-default-zone`. Определила доступные зоны `firewall-cmd --get-zones`. Посмотрела службы, доступные на моём компьютере, используя `firewall-cmd --get-services`. Определила доступные службы в текущей зоне `firewall-cmd --list-services` (рис. 3.1).

```
[root@aazhukoval ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@aazhukoval ~]# 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 bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc
bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb
ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dro
pbox-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
https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos
kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller
kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker
kubernetes kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp
llmnr-udp managesieve matrix mdns memcached minidlna mongod mosh mosh-mount mqt mqtt-tls ms-wbt mssql murmur mysql nbd n
etbios-netbios netdata netdata-dashboard nfs nfs3 nmap-ql38 nre ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-v
mconsole plex pmed pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy
dhcp ps2link ps3netdrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquodad rsh rsyn
cd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission snmp snmptls snmptls-tra
p snmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-
relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsim vnc-s
erver warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp ws
man wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
[root@aazhukoval ~]# firewall-cmd --list-services
cockpit dhcpv6-client ssh
```

Рис. 3.1: Определение текущей зоны по умолчанию, доступной зоны, доступные службы на компьютере, доступные зоны в текущей зоне

2. Сравнила результаты вывода информации при использовании команды `firewall-cmd --list-all` и `firewall-cmd --list-all --zone=public` (рис. 3.2).

```
[root@aaazhukoval ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@aaazhukoval ~]# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@aaazhukoval ~]#
```

Рис. 3.2: Результаты вывода двух команд

3. Добавила сервер VNC в конфигурацию брандмауэра `firewall-cmd --add-service=vnc-server`. Проверила, добавился ли `vnc-server` в конфигурацию (рис. 3.3).

```
[root@aaazhukoval ~]# firewall-cmd --add-service=vnc-server
success
[root@aaazhukoval ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 3.3: Добавление VNC сервера



4. Перезапустила службу firewalld. Проверила, есть ли vnc-server в конфигурации. (рис. 3.4).

```
[root@aazhukoval ~]# systemctl restart firewalld
[root@aazhukoval ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 3.4: Перезапуск службы, проверка наличия сервера

Служба vnc-server больше не указана, так как была не постоянной.

5. Добавила службу vnc-server ещё раз, но на этот раз сделала её постоянной, проверила наличие vnc-server в конфигурации (рис. 3.5).

```
[root@aazhukoval ~]# firewall-cmd --add-service=vnc-server --permanent
success
[root@aazhukoval ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 3.5: Добавление постоянной службы vnc-server

Я увидела, что VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения.

6. Перезагрузила конфигурацию firewalld и просмотрела конфигурацию времени выполнения (рис. 3.6).

```
[root@aazhukoval ~]# firewall-cmd --reload
success
[root@aazhukoval ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 3.6: Перезагрузка конфигурации

7. Добавила в конфигурацию межсетевого экрана порт 2022 протокола TCP, затем перезагрузила конфигурацию firewalld `firewall-cmd --reload`, проверила, что порт добавлен в конфигурацию (рис. 3.7).

```
[root@aazhukoval ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@aazhukoval ~]# firewall-cmd --reload
success
[root@aazhukoval ~]# firewall-cmd --reload
success
[root@aazhukoval ~]# 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:
```

Рис. 3.7: Добавление межсетевого экрана, перезагрузка конфигурации

## 3.2 Управление брандмауэром с помощью firewall-config

1. Открыла терминал и под учётной записью своего пользователя запустила интерфейс GUI firewall-config. Нажала выпадающее меню рядом с параметром Configuration. Открыла раскрывающийся список и выбрала Permanent. Выбрала зону public и отметила службы http, https и ftp, чтобы включить их (рис. 3.8).

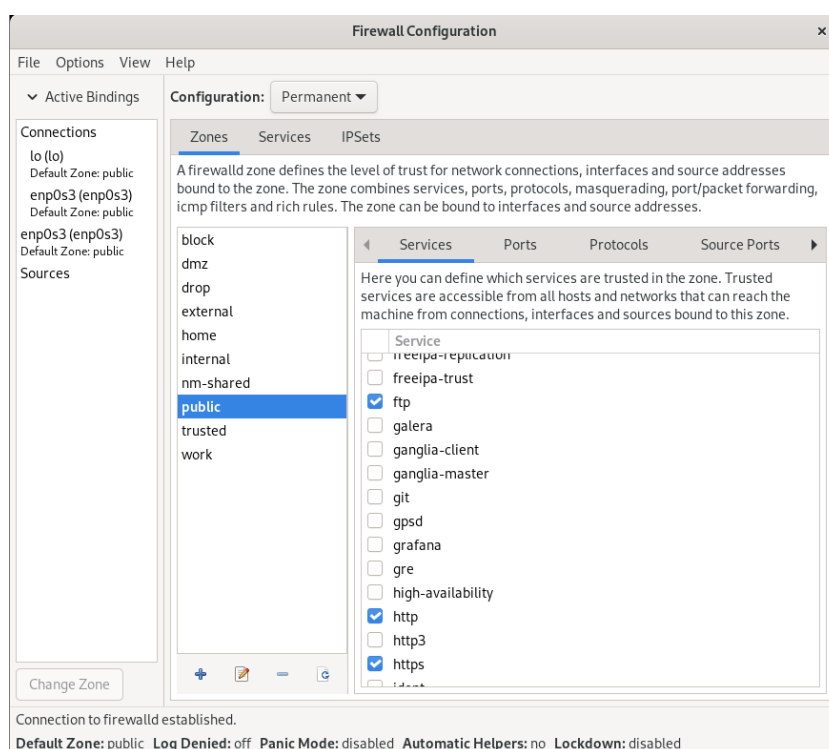


Рис. 3.8: Интерфейс GUI firewall-config

2. Выбрала вкладку Ports и на этой вкладке нажала Add. Ввела порт 2022 и протокол udr, нажала ОК, чтобы добавить их в список (рис. 3.9).

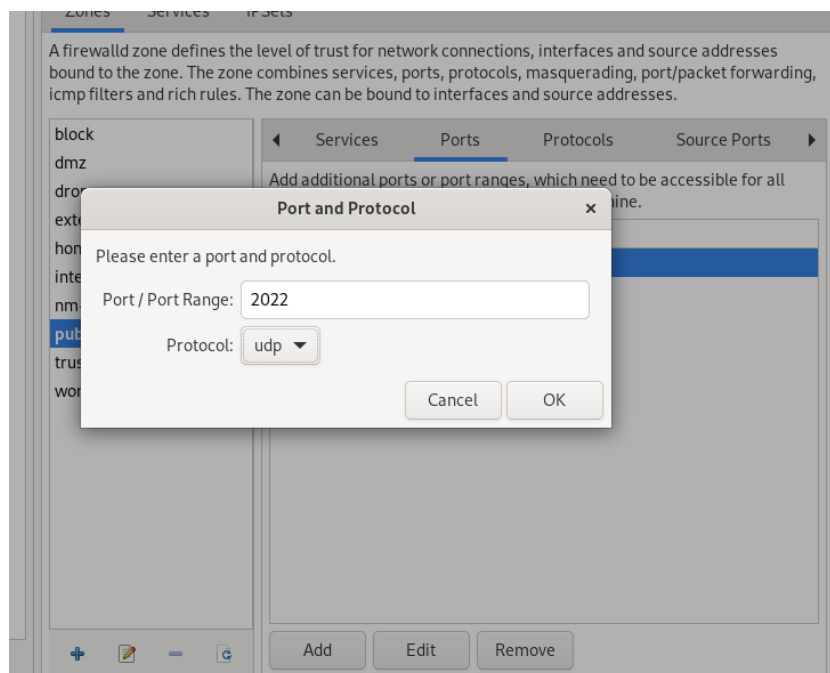


Рис. 3.9: Добавление нового порта

Закрывает утилиту firewall-config.

3. Просмотрела список доступных серверов, перезагрузила конфигурацию firewall-cmd и снова просмотрела список доступных сервисов (рис. 3.10).

```
[aazhukoval@aazhukoval ~]$ 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:
[aazhukoval@aazhukoval ~]$ firewall-cmd --reload
success
[aazhukoval@aazhukoval ~]$ 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:
[aazhukoval@aazhukoval ~]$
```

Рис. 3.10: Проверка подключения серверов

### 3.3 Самостоятельная работа

1. Добавление службы telnet в конфигурацию через терминал. (рис. 3.11).

```
[aazhukoval@aazhukoval ~]$ su -
Password:
[root@aazhukoval ~]# firewall-cmd --add-service=telnet --permanent
success
[root@aazhukoval ~]# firewall-config
Fontconfig error: "/etc/fonts/conf.d/30-0-google-carlito-fonts.conf", line 1:
ocument
```

Рис. 3.11: Добавление службы telnet

2. Создала конфигурацию межсетевого экрана, которая позволяет получить доступ к imap, pop3, smtp в графическом интерфейсе (рис. 3.12).

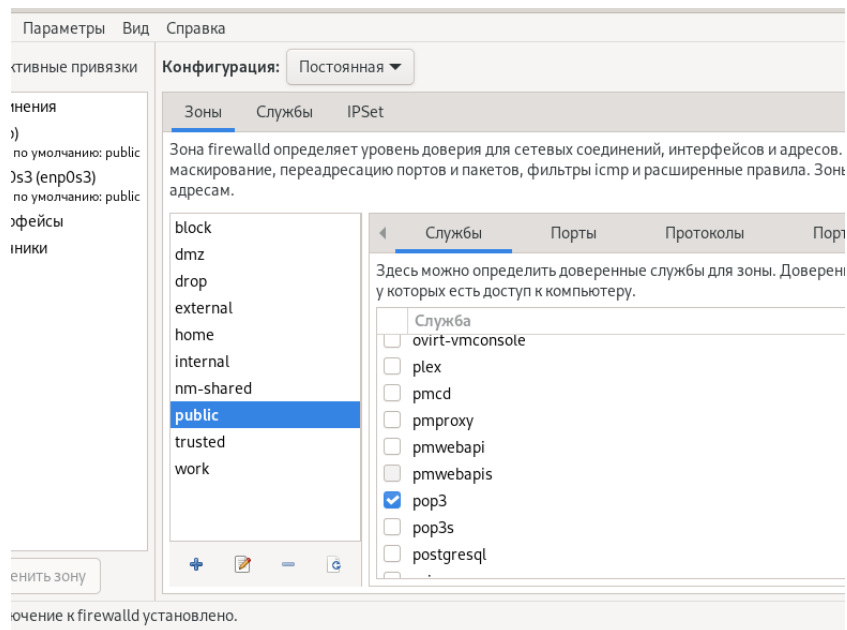


Рис. 3.12: Добавление через графический интерфейс

3. Убедилась, что конфигурация является постоянной и будет активирована после перезагрузки компьютера (рис. 3.13).

```
[root@aazhukoval ~]# firewall-cmd --reload
success
[root@aazhukoval ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ftp http https imap pop3 smtp ssh telnet vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 3.13: Проверка добавления

## 4 Выводы

В ходе выполнения лабораторной работы получила навыки настройки пакетного фильтра в Linux.

## Список литературы

1. Purdy G. N. Linux iptables Pocket Reference. — O'Reilly Media, 2004. — (Pocket Reference).
2. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб. : БХВПетербург, 2011. — (Системный администратор).
3. Vugt S. van. Red Hat RHCSA/RHCE 7 cert guide : Red Hat Enterprise Linux 7 (EX200 and EX300). — Pearson IT Certification, 2016. — (Certification Guide).
4. Динамический брандмауэр с использованием FirewallD. — URL: [https : / / fedoraproject.org/wiki/FirewallD/ru](https://fedoraproject.org/wiki/FirewallD/ru).