

# Отчёт по лабораторной работе №13

## Фильтр пакетов

---

Борисенкова София Павловна

27 ноября 2025

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

## Цель

---

Получить навыки настройки пакетного фильтра и управления брандмауэром в Linux.

## Выполнение лабораторной работы

---

# Получение привилегий

```
root@localhost:/home/spborisenkova/net-adminka/net-admin# su -
Last login: Sat Nov 22 19:48:14 MSK 2025 on pts/0
root@localhost:~# firewall-cmd --get-default-zone
public
root@localhost:~# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@localhost:~# firewall-cmd --get-services
@AD RH-Satellite-6 RH-Satellite-6-capsule afp alvz amanda-client amanda-k5-client amqp amqps anno-1602 anno-18000 apcupsd aseqnet 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 civilization-civilization-v cockpit collected condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpcv6 dhcpcv6-client distcc dnsmasq dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman fo reman-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 iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target ismc jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kpop 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-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft mindlin mmdns mongodb nosh mountn npd mqtt mqtt-tls ns-wbt mssql murmur mysql nbd nbd-client need-for-speed-most-wanted netbios-nx netdata-dashbaord nfs nf3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vnc mconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel roott rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settlers-histroy-collection sip sipr slmevr slp smtp smtp-submission smtpts smtptls smtptls-trap snmptrap spideroak-lansync spotify-sync squid ssdpx ssh statsrv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy sysconsyslog syslog-tls telnet terraria tftp tile38 tinytor socks transmission-client turn turns upnp-client vdsn vnc-server vrpp warpinator wbem-ht tp wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-https wsmans wsmans xdncp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
```

Рис. 1: Определение зоны и служб

## Просмотр зон и служб



The screenshot shows a terminal window with a red header bar. The title bar contains the text "root@localhost:~ - bash" and the path "/net-adminika/net-admin". The terminal window displays the output of the command "firewall-cmd --list-services", which lists services like cockpit, dhcpcv6-client, and ssh. It then shows the output of "firewall-cmd --list-all", which details the configuration for the "public" zone. The configuration includes target (default), ingress and egress priority (0), ICMP block inversion (no), and interfaces (enp0s3). It also lists services (cockpit, dhcpcv6-client, ssh) and ports (forward: yes, masquerade: no, forward-ports, source-ports, icmp-blocks, rich rules). The output concludes with "root@localhost:~#".

```
root@localhost:~# firewall-cmd --list-services
cockpit dhcpcv6-client ssh
root@localhost:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@localhost:~# firewall-cmd --list-all --zone=public
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@localhost:~#
```

Рис. 2: Просмотр конфигурации зоны

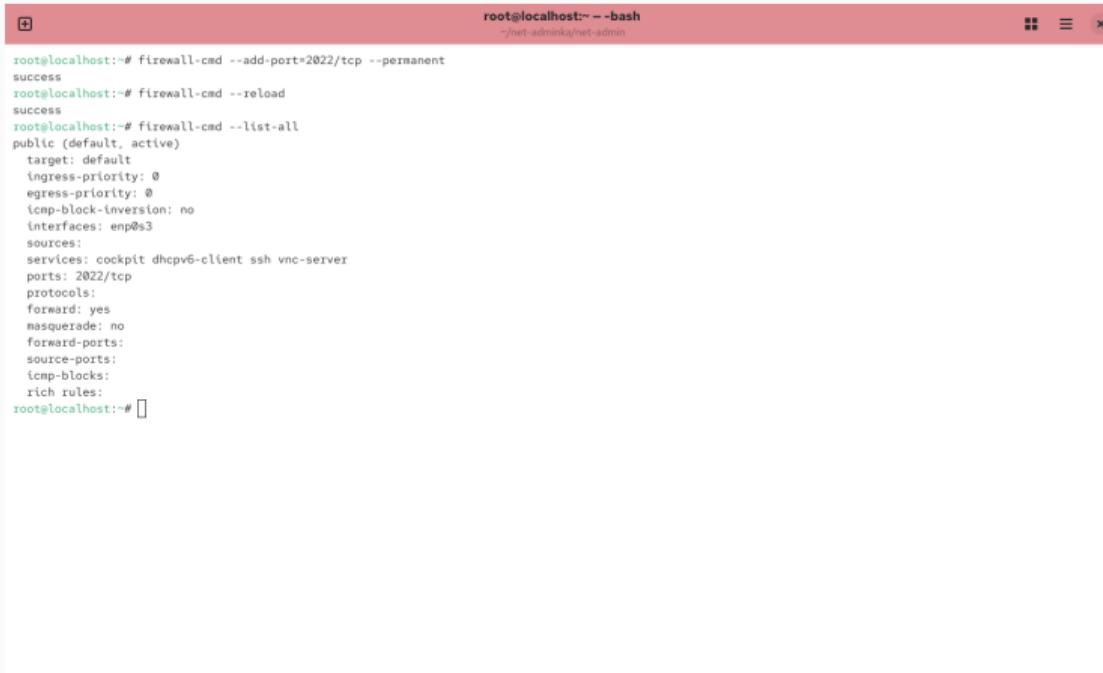
# Добавление службы vnc-server

The screenshot shows a terminal window with a red header bar containing the title 'Добавление службы vnc-server'. The main area of the terminal displays the following command-line session:

```
root@localhost:~# firewall-cmd --add-service=vnc-server
success
root@localhost:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@localhost:~# systemctl restart firewalld
root@localhost:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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:
-----
```

Рис. 3: Добавление vnc-server

## Добавление порта 2022/tcp

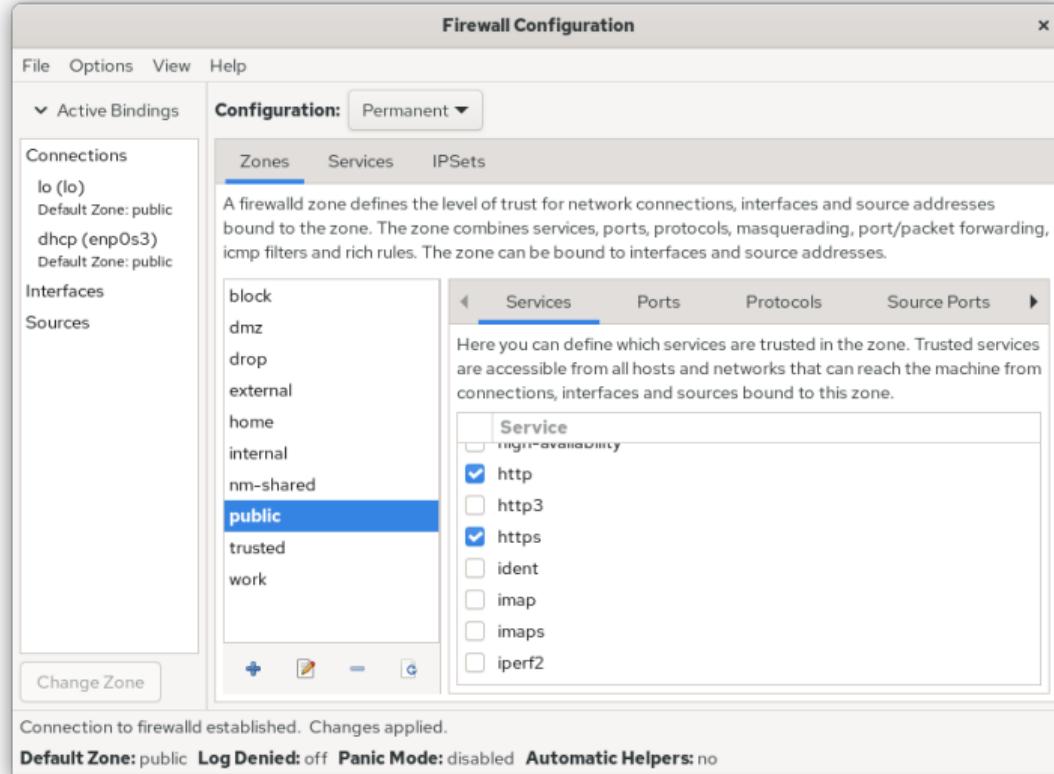


The screenshot shows a terminal window with a red header bar. The title bar reads "root@localhost:~ - bash" and "net-adminka/net-admin". The terminal content is as follows:

```
root@localhost:~# firewall-cmd --add-port=2022/tcp --permanent
success
root@localhost:~# firewall-cmd --reload
success
root@localhost:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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:
  icmp-blocks:
  rich rules:
root@localhost:~#
```

Рис. 4: Добавление порта 2022/tcp

## Запуск firewall-config



# Применение GUI-настроек

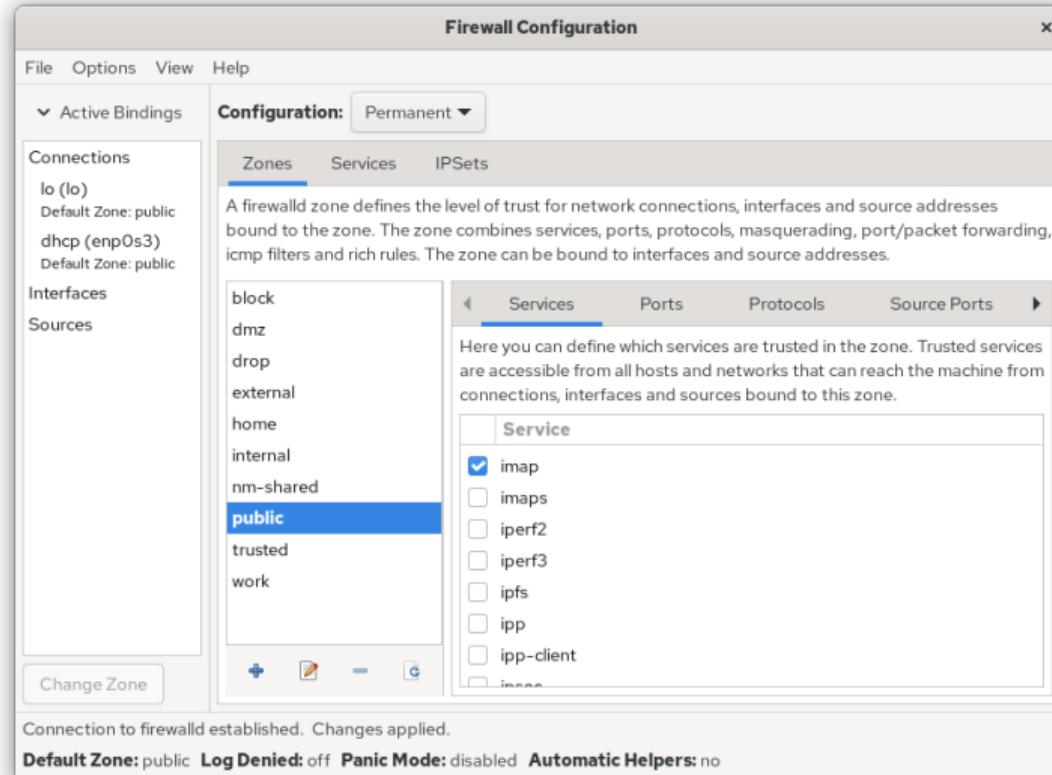


The screenshot shows a terminal window titled "spborisenkova@localhost:~". It displays two command-line sessions. The first session shows the output of the command "firewall-cmd --list-all", which lists a single rule for the "public" target. This rule allows traffic on port 2022/tcp from the "cockpit" service. The second session shows the result of running "firewall-cmd --reload", followed by another "firewall-cmd --list-all" command. This second run shows a new rule that includes "http" and "https" services in addition to "cockpit". The terminal window has a standard Linux-style interface with a title bar, a menu icon, and a close button.

```
spborisenkova@localhost:~$ firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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:
spborisenkova@localhost:~$ firewall-cmd --reload
success
spborisenkova@localhost:~$ firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
    services: cockpit dhcpv6-client ftp http https ssh vnc-server
    ports: 2022/tcp
    protocols:
    forward: yes
    masquerade: no
```

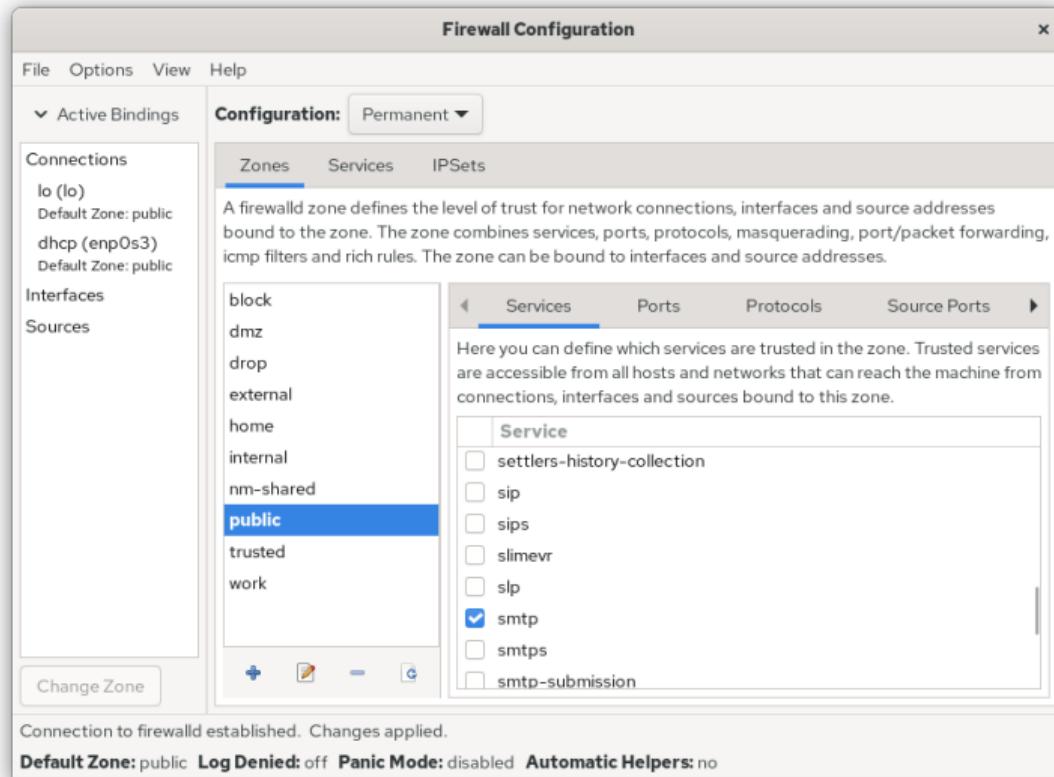
Рис. 6: Применение настроек firewall-config

# Включение imap



## Включение pop3

# Включение smtp



## Итоги работы

---

## Вывод

---

- Изучены механизмы управления firewall через firewall-cmd
- Получены навыки работы с временной и постоянной конфигурацией.
- Освоено добавление служб и портов.
- Применены команды и GUI-инструменты
- Понято различие между runtime и permanent конфигурациями.