

# Лабораторная работа №13

Настройка межсетевого экрана firewalld

---

Анастасия Мазуркевич

07 ноября 2025

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

Получить навыки настройки пакетного фильтра в Linux с использованием `firewalld` и `firewall-config`.

## Ход выполнения

---

# Определение активной зоны

```
admazurkevich@admazurkevich:~$ su
Password:
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# firewall-cmd --get-default-zone
public
root@admazurkevich:/home/admazurkevich# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@admazurkevich:/home/admazurkevich# 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 apcupsd aseqne
t audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-tes
tnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpi
t collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-ov
er-tls docker-registry docker-swarm dropbox-lansync elasticsearch 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 http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenk
ins 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-w
orker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmn
r-udp managesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-mbt mssql murmur mysql n
bd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-im
ageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmpoxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometh
eus-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 s
mtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-tra
nsfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing syncthing-gui syncthi
ng-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns
upnp-client vdsml vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws
-discovery-tcp ws-discovery-udp wsdd wsdd-http wsmann wsmans xdcmcp xmpp-client xmpp-local xmpp-server zabbix-agent zabb
ix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
root@admazurkevich:/home/admazurkevich# █
```

Рис. 1: Информация о зоне и доступных службах

## Просмотр конфигурации зоны

```
root@admazurkevich:/home/admazurkevich# 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
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@admazurkevich:/home/admazurkevich# 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 dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich#
```

## Добавление службы VNC

```
root@admazurkevich:/home/admazurkevich# firewall-cmd --add-service=vnc-server
success
root@admazurkevich:/home/admazurkevich# 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:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@admazurkevich:/home/admazurkevich# systemctl restart firewalld.service
root@admazurkevich:/home/admazurkevich# 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
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@admazurkevich:/home/admazurkevich#
```

## Добавление VNC permanent + reload

```
root@admazurkevich:/home/admazurkevich#  
root@admazurkevich:/home/admazurkevich# firewall-cmd --add-service=vnc-server --permanent  
success  
root@admazurkevich:/home/admazurkevich# 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  
  ports:  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
root@admazurkevich:/home/admazurkevich# firewall-cmd --reload  
success  
root@admazurkevich:/home/admazurkevich# 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:  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:
```



## Добавление TCP-порта 2022

```
root@admazurkevich:/home/admazurkevich#  
root@admazurkevich:/home/admazurkevich# firewall-cmd --add-port=2022/tcp --permanent  
success  
root@admazurkevich:/home/admazurkevich# firewall-cmd --reload  
success  
root@admazurkevich:/home/admazurkevich# 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:  
root@admazurkevich:/home/admazurkevich# █
```

Рис. 5: Добавление порта 2022

# Включение служб http/https/ftp

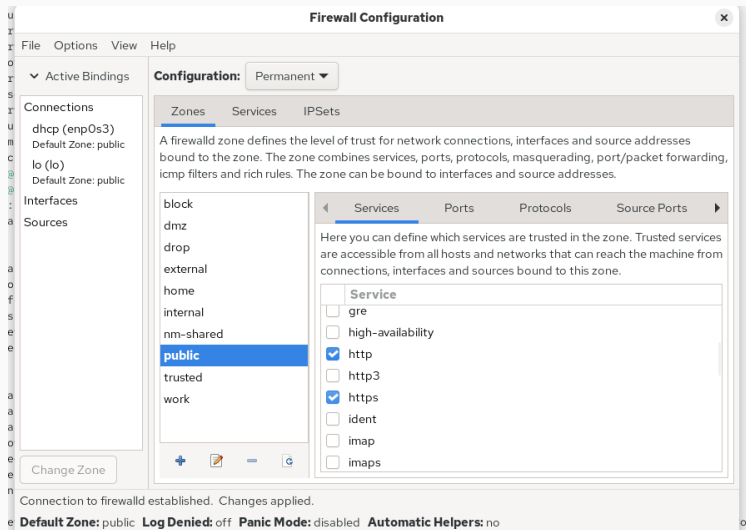


Рис. 6: GUI — включение служб

## Добавление порта 2022/udp

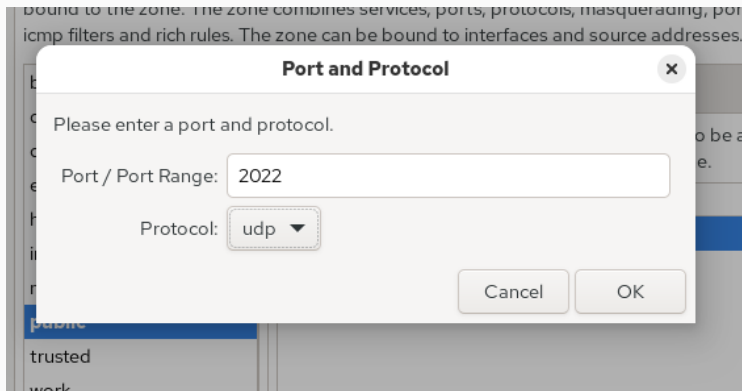


Рис. 7: GUI — добавление порта udp 2022

## Применение изменений (reload)

```
root@admazurkevich:/home/admazurkevich# 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:
root@admazurkevich:/home/admazurkevich# firewall-cmd --reload
success
root@admazurkevich:/home/admazurkevich# 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 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@admazurkevich:/home/admazurkevich#
```

## Добавление служб telnet, imap, pop3, smtp

```
root@admazurkevich:/home/admazurkevich#  
root@admazurkevich:/home/admazurkevich# firewall-cmd --add-service=telnet --permanent  
success  
root@admazurkevich:/home/admazurkevich# firewall-cmd --reload  
success  
root@admazurkevich:/home/admazurkevich# 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 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:  
root@admazurkevich:/home/admazurkevich#
```

Рис. 9: Добавленные службы telnet, imap, pop3, smtp

## Выводы по проделанной работе

---

В ходе лабораторной работы были изучены возможности firewalld: - управление временными и постоянными правилами; - добавление сервисов и портов; - использование терминала и графического интерфейса firewall-config.

Полученные навыки позволяют контролировать сетевой доступ и обеспечивать безопасность системы в Linux.