

# Лабораторная работа №13

Настройка пакетного фильтра (firewalld)

---

Тукаев Тимур

07 ноября 2025

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

Получить практический опыт настройки межсетевого экрана Linux с помощью инструментов `firewall-cmd` и `firewall-config`.

## Ход выполнения

---

# Определение зоны и доступных служб

```
titukaev@titukaev:~$ su
Password:
root@titukaev:/home/titukaev# firewall-cmd --get-default-zone
public
root@titukaev:/home/titukaev# firewall-cmd --get-zones
block dmz drop external home internal no-shared public trusted work
root@titukaev:/home/titukaev# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp aliv amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcupsd aseqnet audit ausweisapp2 bacula bacula-client bareos-director bare
on-filedaemon bareos-storage bb bgp bitcoind bitcoind-rpc bitcoind-testnet bitcoind-testnet-rpc bittorrent-ltd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v
cockpit collectd condor-collector cratedb ctdb dds dds-multicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-qtcp dns-over-tls docker-registry docker-swarm dropbox-lansync ela
sticsearch 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
gssd grafana gre high-availability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadm1n kdeconnect kerberos kibana klogind kpas
smd kprocp 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-sched
uler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managelieve matrix mdns memcache mine
craft minidlna mdp mongodb mosh mountd mpd mqtt mqtt-tls ms-sbt mysql mzsaur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmap-8183 ntp ntpd opente
lemetry openvpn ovirt-inagelo ovirt-storageconsole ovirt-vaconsole plex pfsd pmpoxy pwebapi pwebapi3 pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link
pp3netvrvr ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquoted ssh rsyncd rtp salt-master samba samba-client samba-dc sane settlers-history-col
lection sip sipx slimevr sip setp setp-submission setps snmp snmp1s snmp1s-trap snmptrap spidersnack-lansync spotify-sync squid sddp ssh statdsvr steam-lan-transfer steam-streaming stellaris
stronghold-crusader stun stuns submission supertuxkart svdpd svn syncthing syncthing-gui syncthing-relay synergy syslogd syslog-tls telnet tentacle terraria tfpt tile38 tinc tor-s
ocks transmission-client turn turns upnp-client vdsu vnc-server vrrp waspinator wbes-http wbes-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discove
ry-udp wssd wssd-http wsmans wsmans-xmpp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
root@titukaev:/home/titukaev# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@titukaev:/home/titukaev#
```

Рис. 1: Определение зоны и списка служб

Переход в режим суперпользователя и проверка активной зоны (**public**) и доступных служб/зон в системе.

# Просмотр конфигурации зоны

```
root@titukaev:/home/titukaev#  
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev# 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@titukaev:/home/titukaev#
```

## Добавление службы VNC (временное)

```
root@titukaev:/home/titukaev#  
root@titukaev:/home/titukaev# firewall-cmd --add-service=vnc-server  
success  
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev# systemctl restart firewalld.service  
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev#
```

## Добавление службы VNC (постоянно)

```
root@titukaev:/home/titukaev# firewall-cmd --add-service=vnc-server --permanent
success
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev# firewall-cmd --reload
success
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev#
```



## Добавление порта 2022/tcp

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

Рис. 5: Добавление порта TCP

# Включение служб через GUI

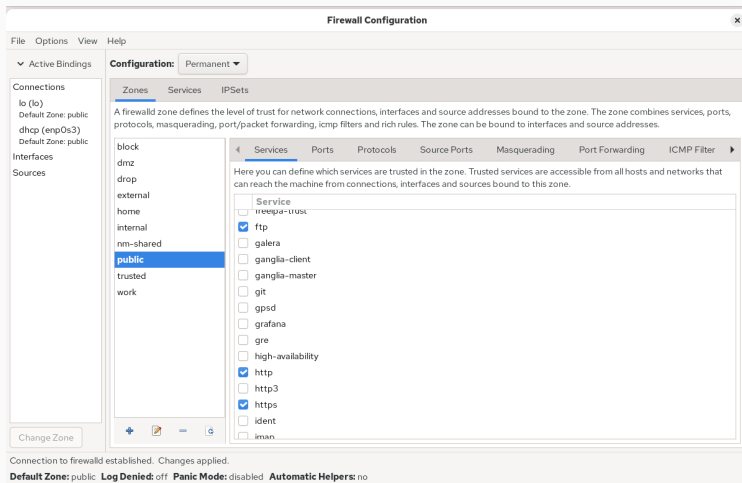


Рис. 6: Включение служб

## Добавление порта через firewall-config

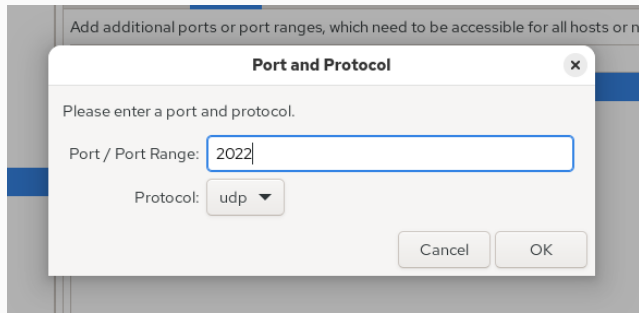


Рис. 7: Добавление порта UDP

Добавление порта 2022/udp через графический интерфейс.

# Применение конфигурации GUI

```
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev# firewall-cmd --reload
success
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev#
```

## Настройка доступа к службам

```
root@titukaev:/home/titukaev#  
root@titukaev:/home/titukaev# firewall-cmd --reload  
success  
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev#
```

Рис. 9: Конфигурация telnet, imap, pop3, smtp

- telnet — добавлен через терминал
- imap, pop3, smtp — добавлены через GUI

## Итоги работы

---

В ходе лабораторной работы освоены:

- настройка межсетевого экрана с помощью `firewall-cmd` и `firewall-config`;
- отличие runtime и permanent конфигураций;
- включение служб и открытие портов;
- управление зонами безопасности.

Полученные навыки позволяют управлять сетевым доступом и обеспечивать безопасность системы.