Отчёт по лабораторной работе №13

Фильтр пакетов (firewalld)

Ришард Когенгар

22 января 2026

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Получить навыки настройки пакетного фильтра в Linux и освоить управление межсетевым экраном **firewalld**: - через командную строку (**firewall-cmd**); - через графический интерфейс (**firewall-config**).

Ход выполнения работы

Управление брандмауэром с помощью firewall-cmd

- Получены полномочия администратора (root)
- Определена зона по умолчанию: **public**
- Просмотрены:
  - доступные зоны
  - доступные службы
  - службы в активной зоне

```
root@rishardkogengar:/home/rishard# firewall-cmd --get-default-zone
public
root@rishardkogengar:/home/rishard# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@rishardkogengar:/home/rishard# 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 aseqnet a
udit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet b
itcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit collect
d condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docke
r-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freei
pa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availabi
lity http http3 https ident imap imaps iperf2 iperf3 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-m
anager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-reado
nly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns
memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wan
ted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmc
onsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps
3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-mast
er samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls snmptl
```

Проверка конфигурации зоны public

- Сравнены результаты:
  - просмотр конфигурации активной зоны
  - просмотр конфигурации явно указанной зоны **public**

```
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# 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:
```

Проверка конфигурации зоны public

- Подтверждено: public является зоной по умолчанию и активной

```
root@rishardkogengar:/home/rishard# 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@rishardkogengar:/home/rishard#
```

Добавление vnc-server во runtime-конфигурацию

- Служба **vnc-server** добавлена в конфигурацию **времени выполнения**
- Проверено наличие службы в списке разрешённых сервисов зоны **public**

```
root@rishardkogengar:/home/rishard# firewall-cmd --add-service=vnc-server
success
root@rishardkogengar:/home/rishard# 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:
```

Сброс runtime-изменений после перезапуска firewalld

- Выполнен перезапуск службы **firewalld**
- Установлено: **vnc-server** исчез из конфигурации
- Причина: изменения были внесены только во **runtime**, без сохранения в **permanent**

```
root@rishardkogengar:/home/rishard# systemctl restart firewalld.service
root@rishardkogengar:/home/rishard# 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:
```

Добавление vnc-server в permanent-конфигурацию

- Служба **vnc-server** добавлена как **permanent**
- Проверка показала: во runtime конфигурации служба не отображается без перезагрузки правил

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

Применение permanent-конфигурации

- Выполнено применение постоянных правил (reload)
- Подтверждено: vnc-server активен в зоне public

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

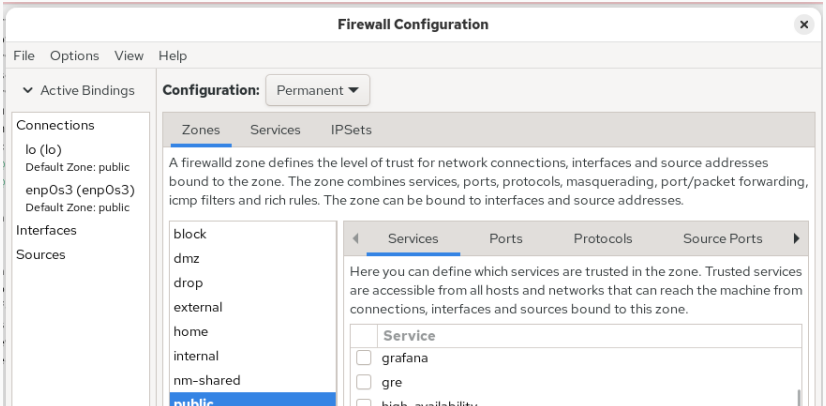
Добавление TCP-порта 2022

- В permanent-конфигурацию добавлен порт **2022/tcp**
- После применения правил подтверждено отображение порта в конфигурации зоны

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

Управление брандмауэром с помощью firewall-config

- Запущена утилита **firewall-config**
- Режим **Configuration: Permanent** выбран для сохранения изменений на диске
- Зона: **public**
- Включены службы: **http**, **https**, **ftp**



Добавление порта 2022/udp в GUI

- На вкладке **Ports** выполнено добавление:
  - Port: **2022**
  - Protocol: **udp**

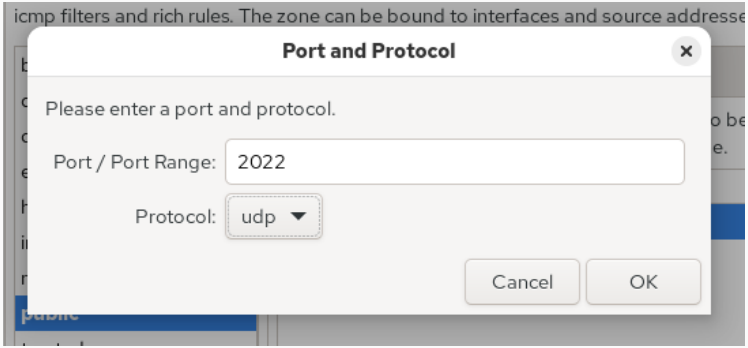


Рис. 10: Добавление 2022/udp через GUI

Проверка: permanent-изменения не активны без reload

- После закрытия firewall-config выполнена проверка конфигурации
- Установлено: изменения ещё не применены к конфигурации времени выполнения

```
root@rishardkogengar:/home/rishard# 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:
```

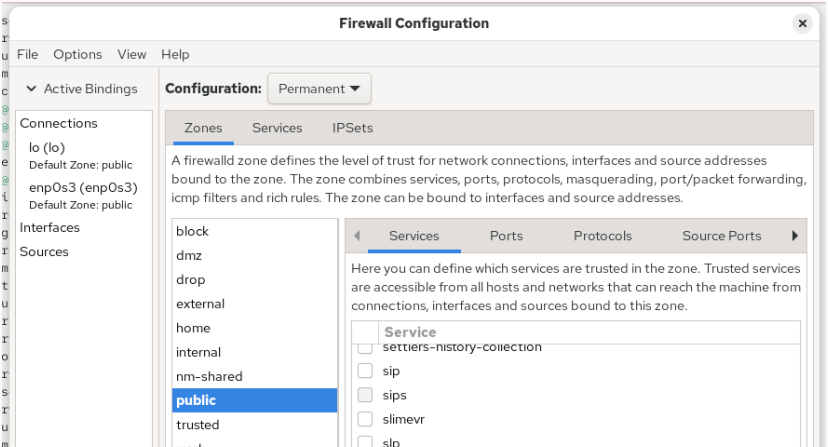
Применение изменений после reload

- Выполнено применение правил
- Подтверждено:
  - службы **http/https/ftp** активны
  - порт **2022/udp** активен

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

Добавление imap/pop3/smtp через GUI

- Зона: **public**
- Режим: **Permanent**
- Отмечены службы: **imap**, **pop3**, **smtp**



Добавление telnet через CLI и итоговая проверка

- telnet добавлен в **permanent**, затем применён (reload)
- Итоговая проверка подтвердила наличие:
  - сервисов (включая telnet, imap, pop3, smtp)
  - портов (2022/tcp, 2022/udp)

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

Итоги работы

Вывод

- Освоены два подхода к управлению firewalld: **firewall-cmd** и **firewall-config**
- Показано различие между:
  - конфигурацией **времени выполнения** (runtime)
  - **постоянной** конфигурацией (permanent)
- Настроена постоянная конфигурация, обеспечивающая доступ к требуемым службам и портам, и корректно применяемая после **reload/перезагрузки**