Лабораторная работа №13

Настройка пакетного фильтра в Linux (firewalld)

Максат Хемраев

5 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Получить навыки работы с брандмауэром **firewalld** и научиться управлять сетевыми правилами через `firewall-cmd` и `firewall-config`.

Ход выполнения работы

Определение зоны по умолчанию

- Проверена зона по умолчанию → **public**
- Просмотрены доступные зоны и список доступных служб

```
mhemraev@mhemraev:~$ su
Password:
root@mhemraev:/home/mhemraev# firewall-cmd --get-default-zone
public
root@mhemraev:/home/mhemraev# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@mhemraev:/home/mhemraev# 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 au
dit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bit
coin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit collectd c
ondor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docker-re
gistry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ld
ap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability h
ttp http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerber
os kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager k
ube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubel
et-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache m
inecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios
-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex
pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp p
ulseaudio 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 smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap
 spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns s
ubmission supertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terrari
a tftp tile38 tinc tor-socks transmission-client turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wiregua
rd ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh
xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
root@mhemraev:/home/mhemraev#
```

Рис. 1: Список зон и служб

Анализ активных правил зоны

- Выведен список разрешённых сервисов в зоне `public`
- Сравнены команды:
  - `firewall-cmd --list-all`
  - `firewall-cmd --list-all --zone=public`

```
root@mhemraev:/home/mhemraev# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@mhemraev:/home/mhemraev# 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@mhemraev:/home/mhemraev# firewall-cmd --list-all --zone=public
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
```

Добавление сервиса VNC (runtime)

- Добавлен сервис **vnc-server** во временную конфигурацию
- Сервис появился в списке разрешённых

```
root@mhemraev:/home/mhemraev#
root@mhemraev:/home/mhemraev# firewall-cmd --add-service=vnc-server
success
root@mhemraev:/home/mhemraev# 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@mhemraev:/home/mhemraev# systemctl restart firewalld.service
root@mhemraev:/home/mhemraev# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
```

Добавление сервиса VNC (permanent)

- Повторное добавление, но теперь *permanent*
- Выполнено `firewall-cmd --reload`
- Сервис стал активным и постоянным

```
root@mhemraev:/home/mhemraev# firewall-cmd --add-service=vnc-server --permanent
success
root@mhemraev:/home/mhemraev# 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@mhemraev:/home/mhemraev# firewall-cmd --reload
success
root@mhemraev:/home/mhemraev# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
```

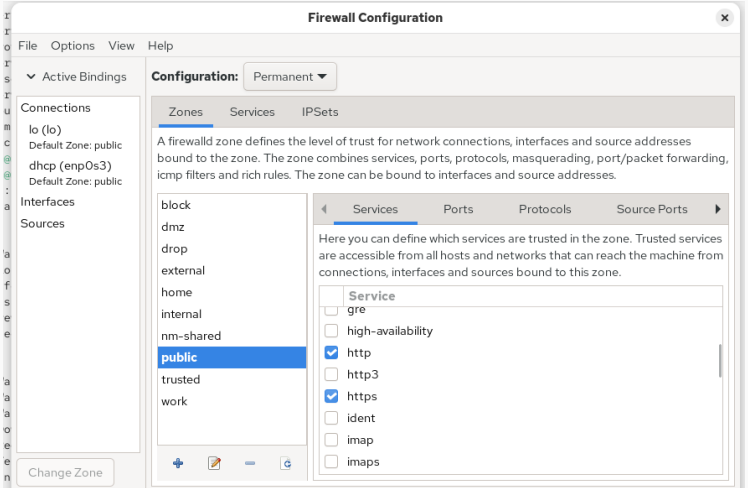
Добавление порта 2022/tcp

- Включён порт **2022/tcp** в постоянную конфигурацию
- Выполнен `firewall-cmd --reload`
- Порт появился в списке активных правил

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

Включение сервисов в firewall-config

- Запущена графическая утилита `firewall-config`
- Активированы сервисы: **http**, **https**, **ftp**



Добавление порта 2022/udp через GUI

- На вкладке *Ports* добавлен порт **2022/udp**

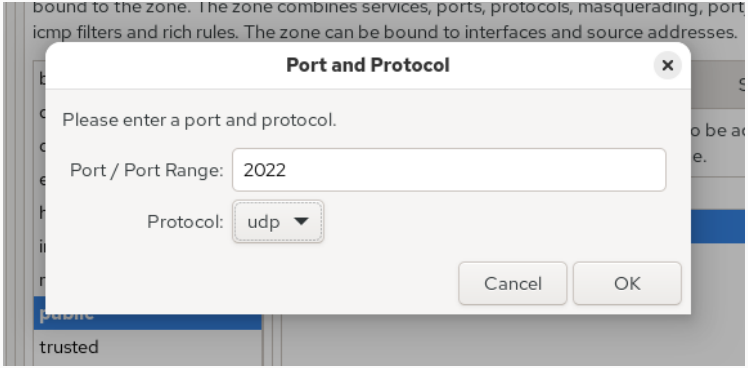


Рис. 7: Добавление порта UDP

Применение настроек

- Для применения постоянных настроек выполнено:
  - `firewall-cmd --reload`
- Все изменения вступили в силу

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

Добавление сетевых сервисов

- Разрешены следующие сервисы:
  - **telnet** — через командную строку
  - **imap**, **pop3**, **smtp** — через firewall-config

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

Рис. 9: Проверка конфигурации

Итоги работы

Вывод

В ходе работы были изучены инструменты **firewalld**,
включая добавление сервисов и портов в *runtime* и *permanent*
конфигурацию, а также настройка правил через `firewall-config`.