Лабораторная работа №13

Фильтр пакетов (firewalld)

Эзиз Хатамов

07 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Получение практических навыков настройки брандмауэра Linux с использованием `firewall-cmd` и `firewall-config`.

Ход выполнения работы

Определение параметров брандмауэра

- Определена зона по умолчанию → **public**
- Просмотрены доступные зоны и список доступных сервисов

```
ehatamov@ehatamov:~$ sudo -i
[sudo] password for ehatamov:
root@ehatamov:~#
root@ehatamov:~# firewall-cmd --get-default-zone
public
root@ehatamov:~# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@ehatamov:~# 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
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-iv civilization-v cockpit coll
ectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls d
ocker-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-av
ailability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kde
connect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-cont
roller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kube
let-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve ma
trix mdns memcache minecraft mindidna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-spe
ed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconso
le ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dh
cp 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 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 submission supertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog
syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-client vdsm vnc-server vrrp war
pinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd w
sdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-tra
pper zabbix-web-service zero-k zerotier
root@ehatamov:~#
```

Проверка активных сервисов

- Просмотрены сервисы, разрешённые в зоне `public`
- Сравнение `--list-all` и `--list-all --zone=public`
- Зона `public` является зоной по умолчанию

```
root@ehatamov:~# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@ehatamov:~# 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@ehatamov:~# firewall-cmd --list-all --zone=public
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
```

Добавление сервиса VNC (runtime)

- Добавлен сервис: `vnc-server`
- Проверено наличие сервиса — отображается

```
root@ehatamov:~# firewall-cmd --add-service=vnc-server
success
root@ehatamov:~# 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@ehatamov:~# systemctl restart firewalld.service
root@ehatamov:~# 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:
```

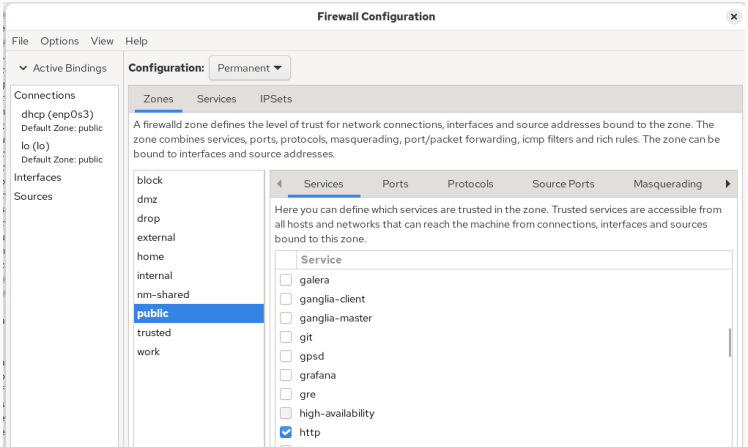
Добавление сервиса VNC (permanent)

- Добавлен как постоянный (`--permanent`)
- Для применения настроек выполнен `firewall-cmd --reload`
- Сервис появился в списке активных

```
root@ehatamov:~# firewall-cmd --add-service=vnc-server --permanent
success
root@ehatamov:~# 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@ehatamov:~# firewall-cmd --reload
success
root@ehatamov:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
```

Используем графический интерфейс

- Запущено приложение `firewall-config`
- Выбрана конфигурация **Permanent**
- В зоне `public` включены сервисы: `http`, `https`, `ftp`



Добавление порта через GUI

- На вкладке *Ports* добавлен: `2022/udp`
- После `firewall-cmd --reload` порт стал активен

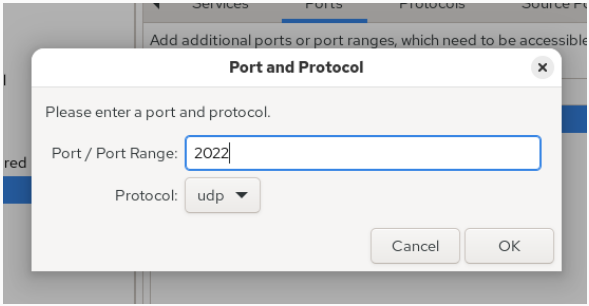
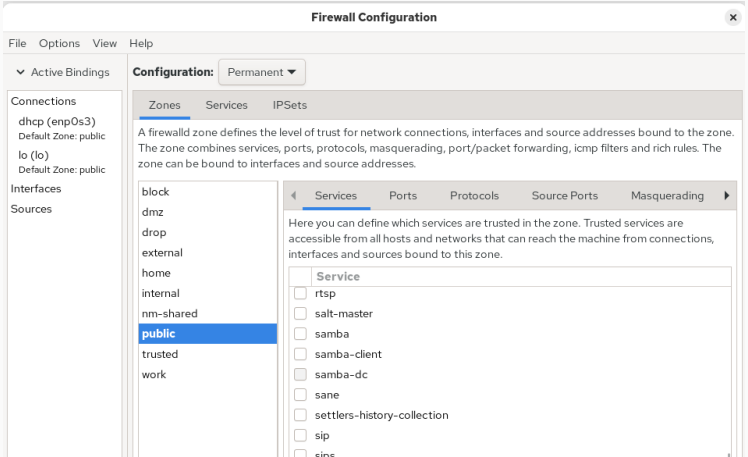


Рис. 6: GUI: добавление порта

Добавление сервисов доступа

- Добавлено:
  - `telnet` — через командную строку
  - `imap`, `pop3`, `smtp` — через GUI



Все службы добавлены корректно

- Конфигурация стала постоянной

```
root@ehatamov:~#
root@ehatamov:~# firewall-config
root@ehatamov:~#
root@ehatamov:~# firewall-cmd --add-service=telnet
success
root@ehatamov:~# firewall-cmd --add-service=telnet --permanent
success
root@ehatamov:~# firewall-cmd --reload
success
root@ehatamov:~# 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@ehatamov:~#
```

Рис. 8: Финальная конфигурация

Вывод

Итоги выполнения работы

- Изучены команды `firewall-cmd` и принципы runtime/permanent конфигураций
- Освоено добавление сервисов и портов (CLI + GUI)
- Получены навыки управления зонами и сетевыми разрешениями в Linux