Лабораторная работа №13

Фильтр пакетов (firewalld)

Сулейм Гамбердов

07 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Получить навыки настройки пакетного фильтра Linux с помощью инструментов:

- **firewall-cmd** (CLI)
- **firewall-config** (GUI)

Ход выполнения

Определение параметров брандмауэра

```
root@sigamberdov:/home/sigamberdov# firewall-cmd --get-default-zone
public
root@sigamberdov:/home/sigamberdov# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@sigamberdov:/home/sigamberdov# 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-storag
e 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 collectd condor-collector cratedb ctdb dds dds
-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docker-registry docke
r-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 jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api k
ube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-s
ecure 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 managesiev
e matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mys
ql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opente
lemetry 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 pulseaudio pu
ppetmaster 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 smtp
s snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfe
r steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing synct
hing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-s
ocks 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 za
bbix-trapper zabbix-web-service zero-k zerotier
root@sigamberdov:/home/sigamberdov# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@sigamberdov:/home/sigamberdov#
```

Просмотр настроек зоны

```
root@sigamberdov:/home/sigamberdov# 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@sigamberdov:/home/sigamberdov# 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:
```

Добавление сервиса (runtime)

Сервис VNC добавлен во временную конфигурацию.

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

Перезагрузка и потеря изменений

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


Рис. 4: После перезапуска службы vnc-server исчезает

Добавление сервиса (permanent)

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

Рис. 5: Добавление сервиса permanently

Активация постоянной конфигурации

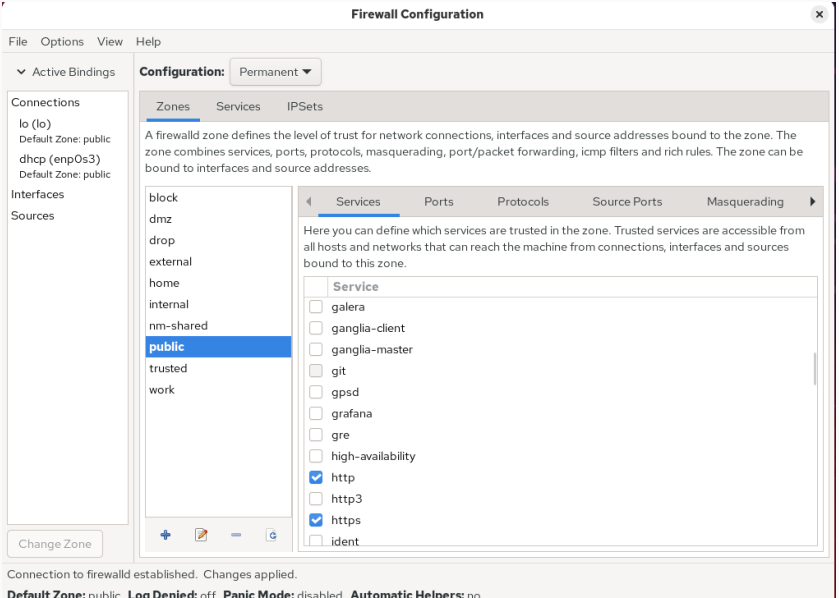
```
root@sigamberdov:/home/sigamberdov# firewall-cmd --reload
success
root@sigamberdov:/home/sigamberdov# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@sigamberdov:/home/sigamberdov#
```

Добавление портов

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


Рис. 7: Добавление порта 2022

Выбор режима Permanent



Добавление порта через GUI

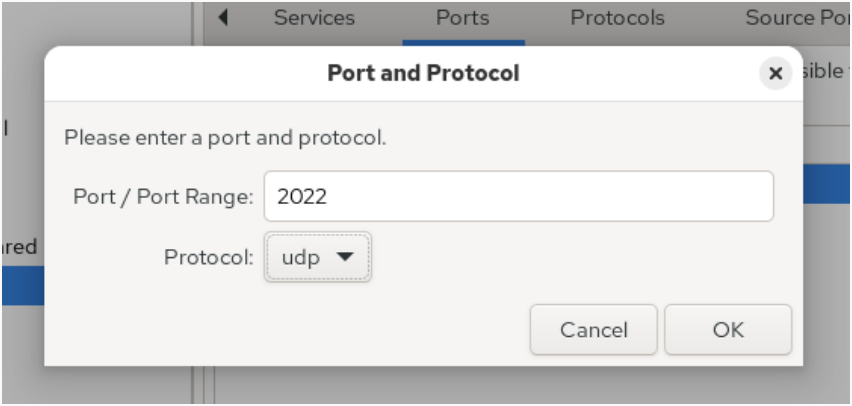


Рис. 9: Добавление порта 2022/udp

Активация изменений

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

Выполненные действия

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


Рис. 11: Итоговая конфигурация

Заключение

Вывод

В ходе работы были освоены:

- управление брандмауэром через **CLI и GUI**
- добавление и удаление служб и портов
- различие между runtime и permanent конфигурациями

Получены практические навыки администрирования сетевой безопасности в Linux.