Лабораторная работа №13

Фильтр пакетов. Управление брандмауэром firewalld

Лабси Мохаммед

07 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Получить навыки настройки пакетного фильтра в Linux с использованием **firewall-cmd** и **firewall-config**.

Ход выполнения

Управление через firewall-cmd

```
mlabsi@mlabsi:~$ su
Password:
root@mlabsi:/home/mlabsi# firewall-cmd --get-default-zone
public
root@mlabsi:/home/mlabsi# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@mlabsi:/home/mlabsi# firewall-cmd --get-services '
> ^C
root@mlabsi:/home/mlabsi# 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 apcups
d 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 collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client
 distcc dns dns-over-quic dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-serve
r factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galer
a ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https ident imap imaps iperf2 iperf3 i
pfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshel
l kube-api kube-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 kubelet-worker ld
ap 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-wa
nted 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-exporte
r proxy-dhcp 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 s
mtp 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 synct
hing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmi
ssion-client turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-disco
very-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@mlabsi:/home/mlabsi#
```

Рис. 1: Просмотр зон

Просмотр доступных сервисов

```
root@mlabsi:/home/mlabsi# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@mlabsi:/home/mlabsi# 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@mlabsi:/home/mlabsi# 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@mlabsi:/home/mlabsi#
```

Добавление сервиса VNC

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

Рис. 3: Добавление VNC-сервера

Перезапуск службы firewalld

```
root@mlabsi:/home/mlabsi#
root@mlabsi:/home/mlabsi# systemctl restart firewalld
root@mlabsi:/home/mlabsi# 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@mlabsi:/home/mlabsi#
```

Рис. 4: VNC отсутствует после перезапуска

Добавление vnc-server постоянно

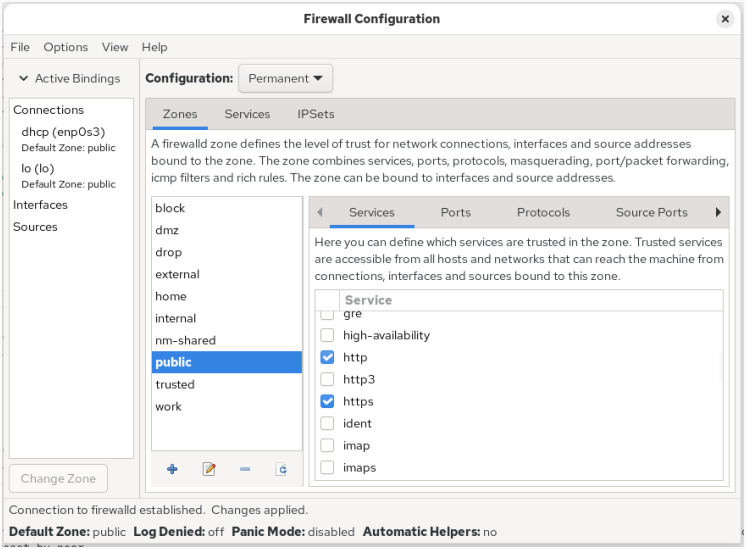
```
root@mlabsi:/home/mlabsi#
root@mlabsi:/home/mlabsi# firewall-cmd --add-service=vnc-server --permanent
success
root@mlabsi:/home/mlabsi# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@mlabsi:/home/mlabsi# firewall-cmd --reload
success
root@mlabsi:/home/mlabsi# 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 порта 2022

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

Рис. 6: Добавление порта 2022

Включение сервисов в GUI



Добавление порта через GUI

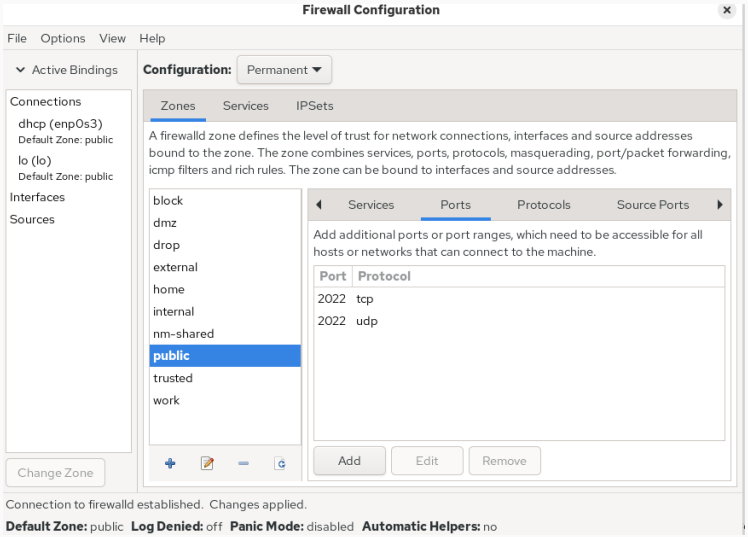


Рис. 8: Добавление порта 2022 UDP

Применение конфигурации

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

Добавление дополнительных служб

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

Рис. 10: Службы добавлены

Заключение

Заключение

В ходе работы были получены практические навыки:

- управления сетевой фильтрацией с использованием **firewall-cmd**;
- добавления сервисов и портов во временную и постоянную конфигурацию;
- использования графического интерфейса **firewall-config**.

Получены важные навыки администрирования сетевой безопасности в Linux.