Презентация по лабораторной работе №13

Настройка пакетного фильтра (firewalld)

Анна Саенко

6 ноября 2025 г.

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Получить практические навыки работы с брандмауэром Linux и конфигурацией пакетного фильтра с использованием `firewall-cmd` и `firewall-config`.

Задачи лабораторной работы

1 Определить активную зону и доступные службы

2 Добавить сервис в runtime и permanent конфигурации

3 Добавить порт TCP/UDP в зону

4 Изменить конфигурацию через GUI (`firewall-config`)

5 Проверить применение изменений

Ход выполнения работы

Определение активной зоны и доступных служб

```
aasaenko@aasaenko:~$ su
Password:
root@aasaenko:/home/aasaenko# firewall-cmd --get-default-zone
public
root@aasaenko:/home/aasaenko# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@aasaenko:/home/aasaenko# 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 ausweis
app2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bitto
rrent-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 elastics
earch 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 kube-apiserver kube-control-pl
ane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secur
e kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp m
anagesieve matrix mdns memcache minecraft minidlna 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-storageconsole ovirt-vmco
nsole 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 sam
ba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spo
tify-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-cl
ient turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host w
s-discovery-tcp ws-discovery-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gatewa
y zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
root@aasaenko:/home/aasaenko# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@aasaenko:/home/aasaenko#
```

Рис. 1: Получение информации о зонах и сервисах

Просмотр текущей конфигурации зоны

```
root@aasaenko:/home/aasaenko# 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@aasaenko:/home/aasaenko# 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@aasaenko:/home/aasaenko#
```

Добавление сервиса vnc-server (runtime)

```
root@aasaenko:/home/aasaenko# firewall-cmd --add-service=vnc-server
success
root@aasaenko:/home/aasaenko# 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@aasaenko:/home/aasaenko# systemctl restart firewalld.service
root@aasaenko:/home/aasaenko# 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@aasaenko:/home/aasaenko#
```

Добавление сервиса vnc-server (permanent)

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

Добавление порта 2022/TCP

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

Рис. 5: Добавление порта 2022

Включение служб (ftp, http, https)

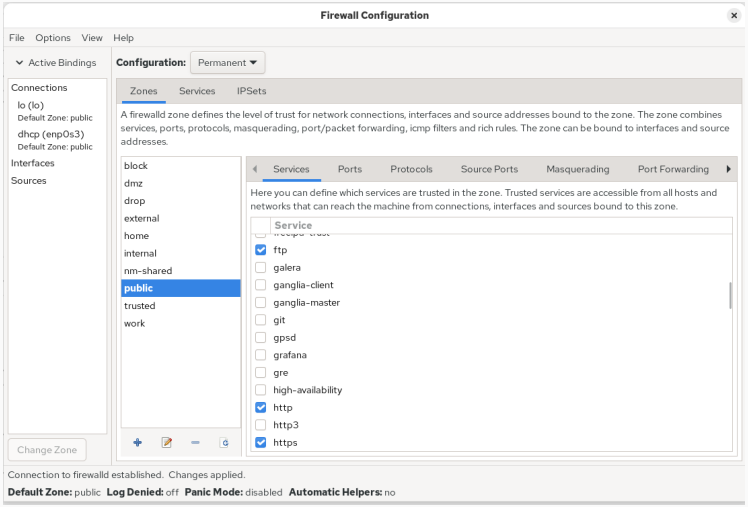

Рис. 6: Добавление служб через GUI

Добавление порта 2022/udp

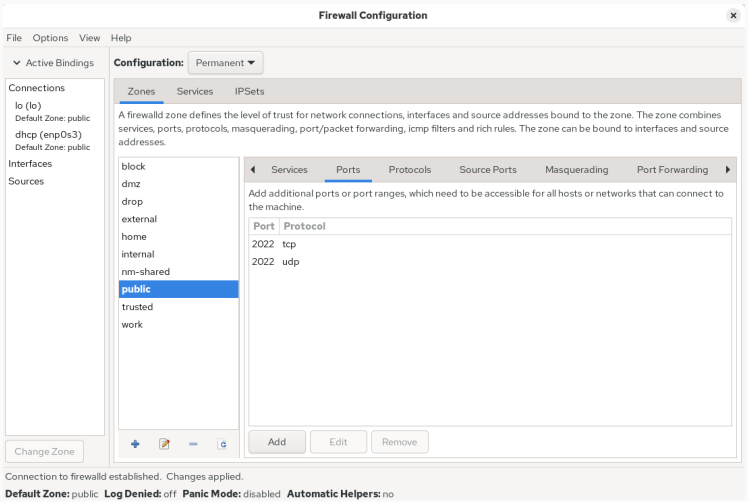

Рис. 7: Добавление порта через GUI

Настройка служб telnet, imap, pop3, smtp

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

Рис. 8: Финальная конфигурация

Выводы

В ходе лабораторной работы были выполнены:

- просмотр и анализ текущей зоны и служб;
- добавление сервиса в runtime и permanent конфигурации;
- объяснение различий между временными и постоянными настройками;
- добавление сетевых портов;
- использование GUI `firewall-config` для управления службами.