Лабораторная работа №13

Фильтр пакетов (firewalld)

Шаханеоядж Хаоладар

2025

Российский университет дружбы народов, Москва, Россия

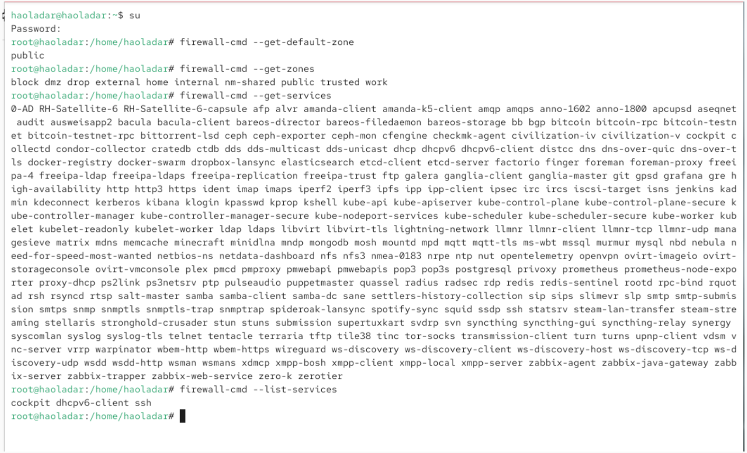
Цель работы

Основная цель

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

Ход выполнения работы

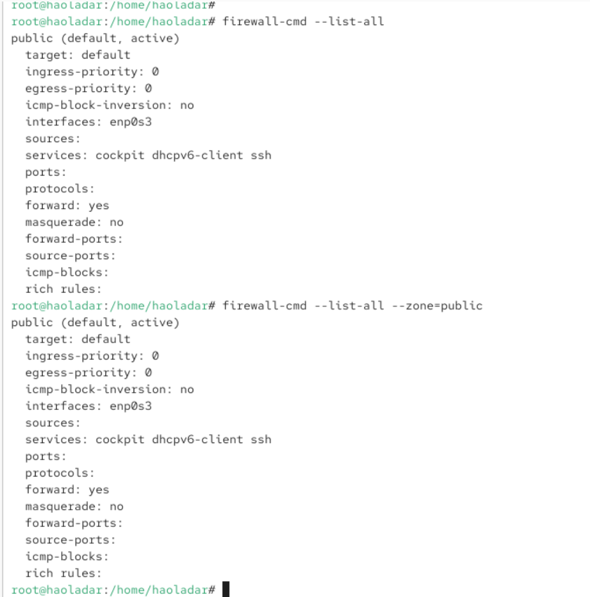
Определение активной зоны



```
haoladar@haoladar:~$ su
Password:
root@haoladar:/home/haoladar# firewall-cmd --get-default-zone
public
root@haoladar:/home/haoladar# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@haoladar:/home/haoladar# 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-testn
et bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit c
ollectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-t
ls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freei
pa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre h
igh-availability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kad
min kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure k
ube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kub
elet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp mana
gesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula n
eed-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-expo
rter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquot
ad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submis
sion smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfer steam-stre
aming 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 v
nc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-d
iscovery-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabb
ix-server zabbix-trapper zabbix-web-service zero-k zerotier
root@haoladar:/home/haoladar# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@haoladar:/home/haoladar# 
```

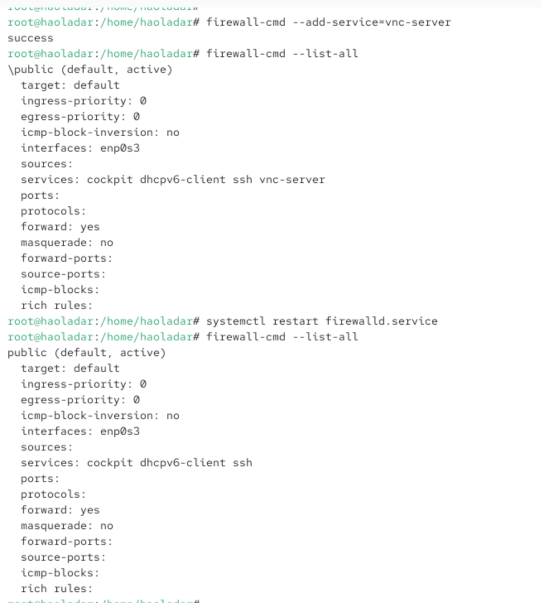
Рис. 1: Список сервисов

Просмотр параметров зоны



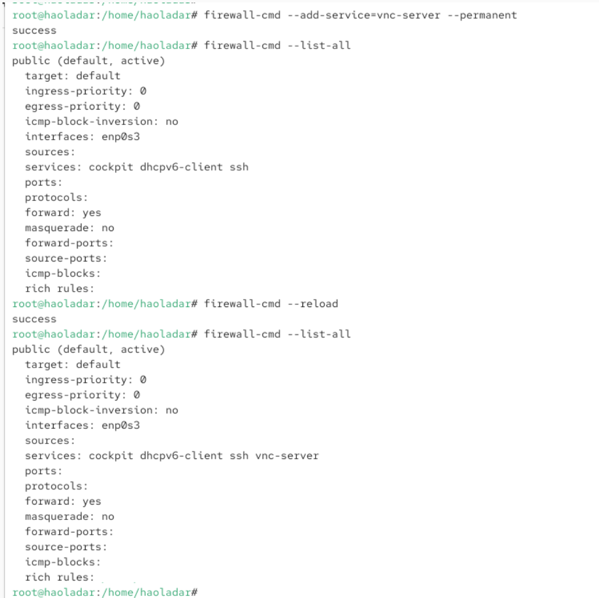
```
root@haoladar:/home/haoladar#
root@haoladar:/home/haoladar# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: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

Добавление сервиса (runtime)



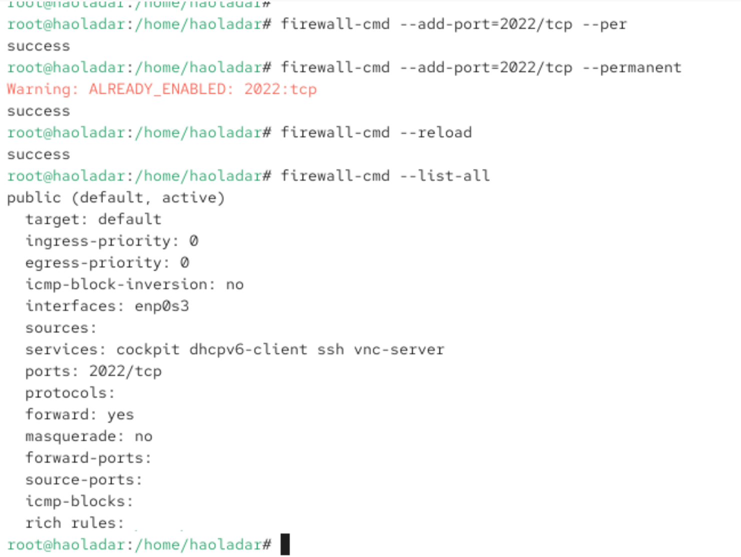
```
root@haoladar:/home/haoladar#
root@haoladar:/home/haoladar# firewall-cmd --add-service=vnc-server
success
root@haoladar:/home/haoladar# firewall-cmd --list-all
\public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
 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

Добавление сервиса (permanent)



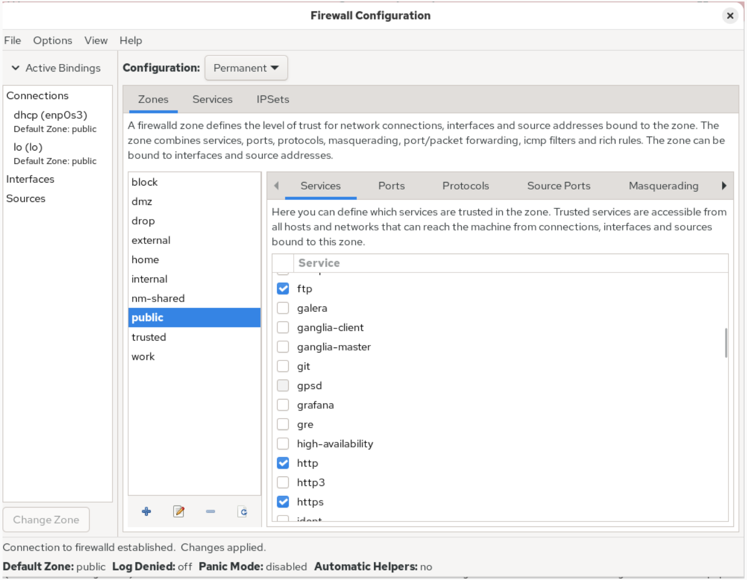
```
root@haoladar:/home/haoladar# firewall-cmd --add-service=vnc-server --permanent
success
root@haoladar:/home/haoladar# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: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

Добавление порта



```
root@haoladar:/home/haoladar#
root@haoladar:/home/haoladar# firewall-cmd --add-port=2022/tcp --per
success
root@haoladar:/home/haoladar# firewall-cmd --add-port=2022/tcp --permanent
Warning: ALREADY_ENABLED: 2022:tcp
success
root@haoladar:/home/haoladar# firewall-cmd --reload
success
root@haoladar:/home/haoladar# 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@haoladar:/home/haoladar# 
```

Выбор режима конфигурации



Configuration: Permanent

A firewalld zone defines the level of trust for network connections, interfaces and source addresses bound to the zone. The zone combines services, ports, protocols, masquerading, port/packet forwarding, icmp filters and rich rules. The zone can be bound to interfaces and source addresses.

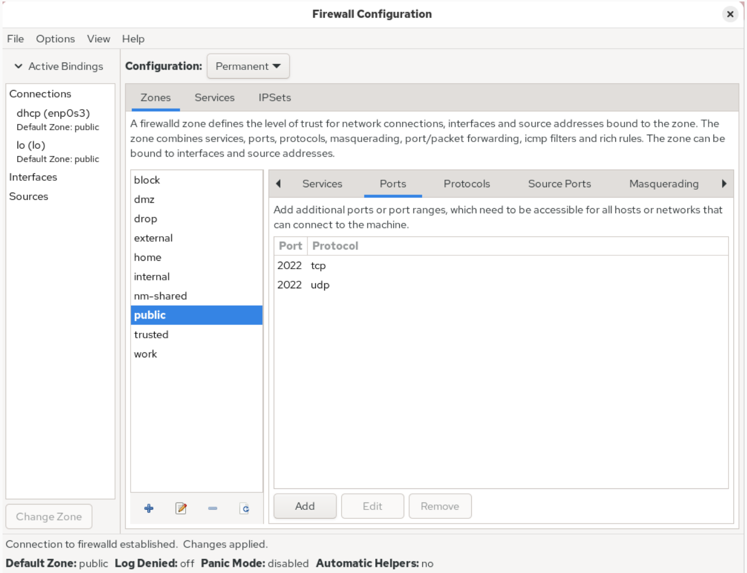
Here you can define which services are trusted in the zone. Trusted services are accessible from all hosts and networks that can reach the machine from connections, interfaces and sources bound to this zone.

- ☑ ftp
- □ galera
- □ ganglia-client
- □ ganglia-master
- □ git
- □ gpsd
- □ grafana
- □ gre
- □ high-availability
- ☑ http
- □ http3
- ☑ https

Connection to firewalld established. Changes applied.

Default Zone: public **Log Denied:** off **Panic Mode:** disabled **Automatic Helpers:** no

Добавление порта через GUI



Connections

dhcp (enp0s3)
Default Zone: public

lo (lo)
Default Zone: public

Interfaces

Sources

A firewalld zone defines the level of trust for network connections, interfaces and source addresses bound to the zone. The zone combines services, ports, protocols, masquerading, port/packet forwarding, icmp filters and rich rules. The zone can be bound to interfaces and source addresses.

- block
- dmz
- drop
- external
- home
- internal
- nm-shared
- public
- trusted
- work

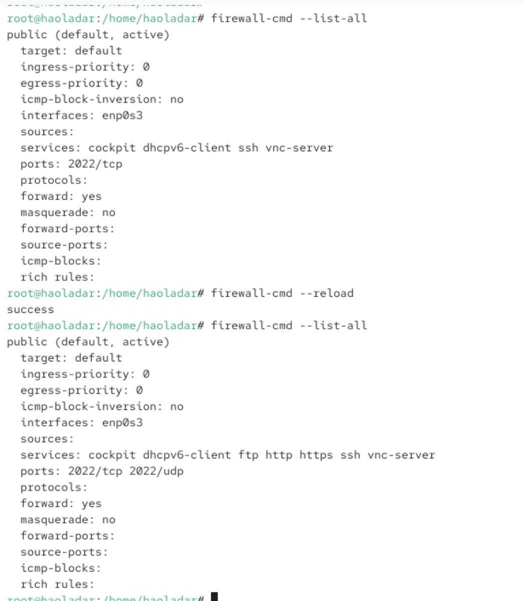
Add additional ports or port ranges, which need to be accessible for all hosts or networks that can connect to the machine.

Port	Protocol
2022	tcp
2022	udp

Connection to firewalld established. Changes applied.

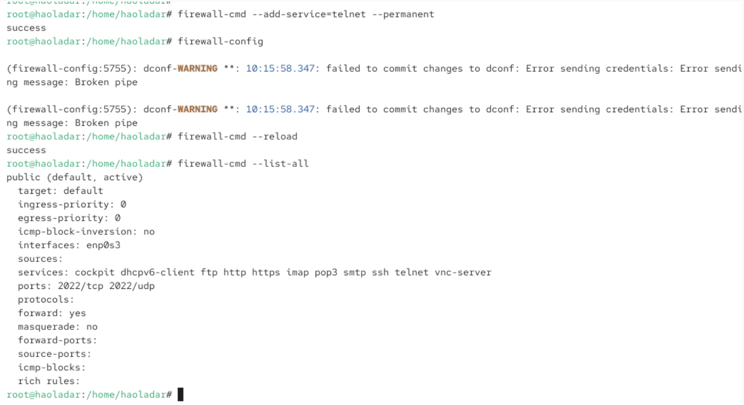
Default Zone: public **Log Denied:** off **Panic Mode:** disabled **Automatic Helpers:** no

Применение конфигурации



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

Добавление служб



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

(firewall-config:5755): dconf-WARNING **: 10:15:58.347: failed to commit changes to dconf: Error sending credentials: Error sendi
ng message: Broken pipe

(firewall-config:5755): dconf-WARNING **: 10:15:58.347: failed to commit changes to dconf: Error sending credentials: Error sendi
ng message: Broken pipe
root@haoladar:/home/haoladar# firewall-cmd --reload
success
root@haoladar:/home/haoladar# 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@haoladar:/home/haoladar# 
```

Рис. 9: Итоговая конфигурация

Итоги работы

Вывод

- Изучено управление брандмауэром через **firewall-cmd** и **firewall-config**
- Получены навыки добавления сервисов и портов
- Освоено применение временных и постоянных правил
- Выполнено управление зонами и интерфейсами в Linux