Презентация по лабораторной работе №13

Фильтр пакетов (firewalld)

Агджабекова Эся Рустамовна

05 ноября 2025

Российский университет дружбы народов, Москва, Россия

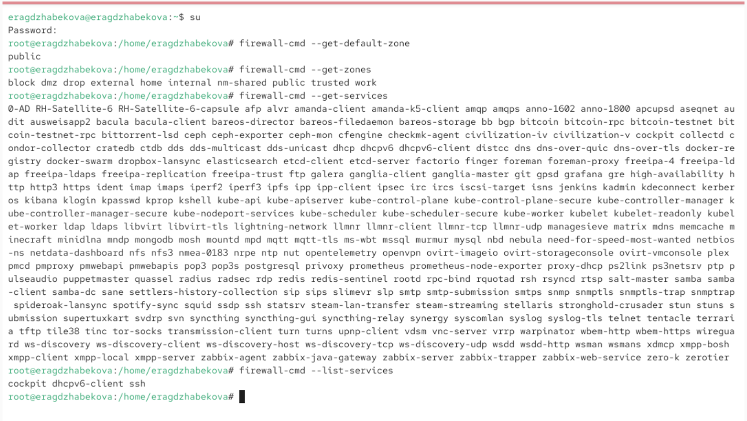
Цель работы

Цель работы

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

Ход выполнения работы

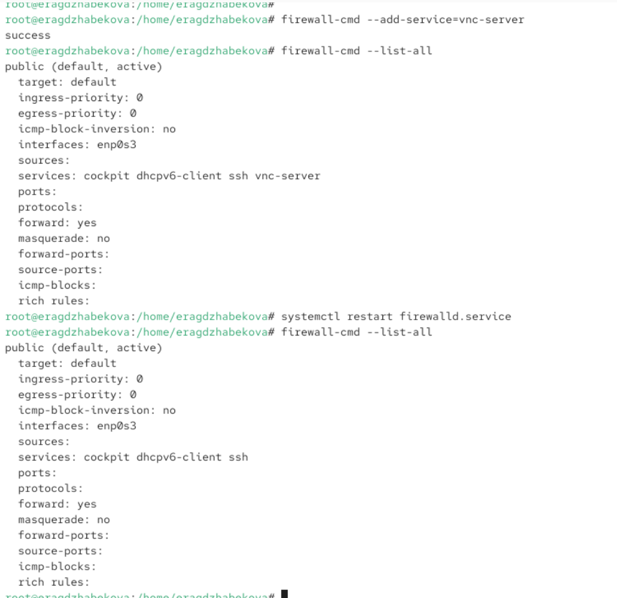
Управление брандмауэром с помощью firewall-cmd



```
eragdzhabekova@eragdzhabekova:~$ su
Password:
root@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --get-default-zone
public
root@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@eragdzhabekova:/home/eragdzhabekova# 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 au
dit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bit
coin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit collectd c
ondor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docker-re
gistry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ld
ap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability h
ttp http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerber
os kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager k
ube-controller-manager-secure 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 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-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-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 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 s
ubmission supertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terrari
a tftp tile38 tinc tor-socks 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 zabbix-trapper zabbix-web-service zero-k zerotier
root@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@eragdzhabekova:/home/eragdzhabekova# █
```

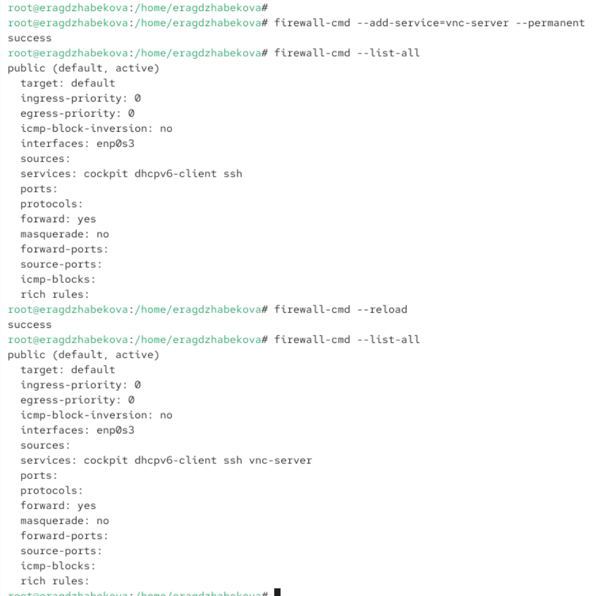
Рис. 1: Определение зоны и доступных сервисов

Временное добавление сервиса



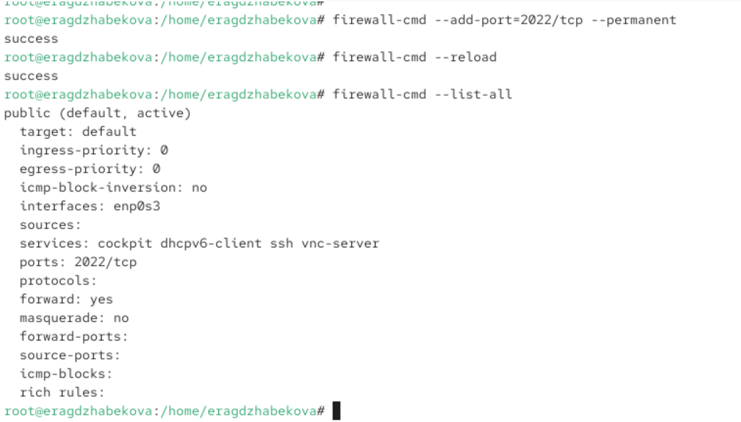
```
root@eragdzhabekova:/home/eragdzhabekova#
root@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --add-service=vnc-server
success
root@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: 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@eragdzhabekova:/home/eragdzhabekova# systemctl restart firewalld.service
root@eragdzhabekova:/home/eragdzhabekova# 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@eragdzhabekova:/home/eragdzhabekova# 
```

Добавление сервиса в постоянную конфигурацию



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

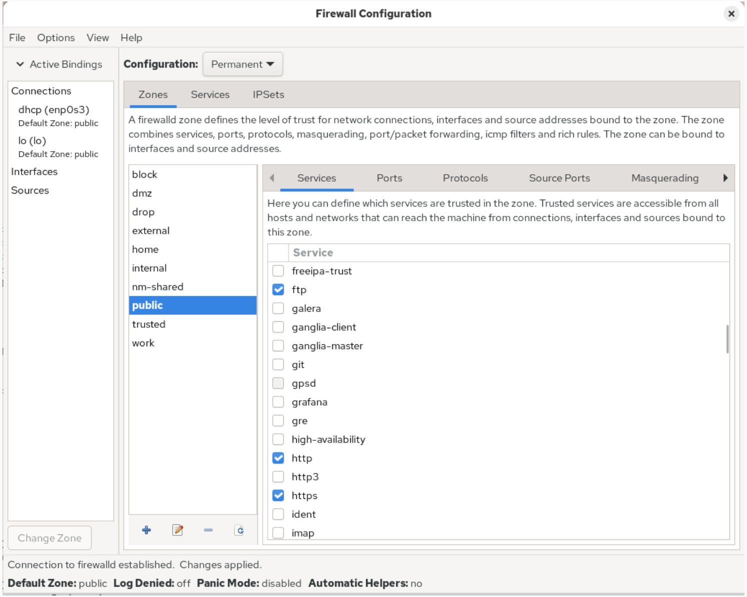
Добавление порта



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

Рис. 4: Добавление порта 2022/tcp

Настройка постоянной конфигурации


Firewall Configuration

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

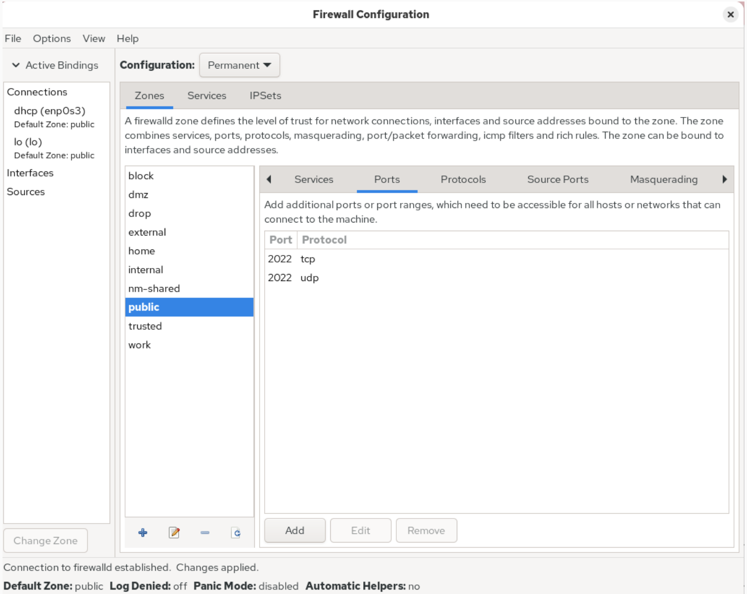
Here you can define which services are trusted in the zone. Trusted services are accessible from all hosts and networks that can reach the machine from connections, interfaces and sources bound to this zone.

	Service
□	freeipa-trust
☑	ftp
□	galera
□	ganglia-client
□	ganglia-master
□	git
□	gpsd
□	grafana
□	gre
□	high-availability
☑	http
□	http3
☑	https
□	ident
□	imap

Connection to firewalld established. Changes applied.

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

Добавление порта через GUI



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.

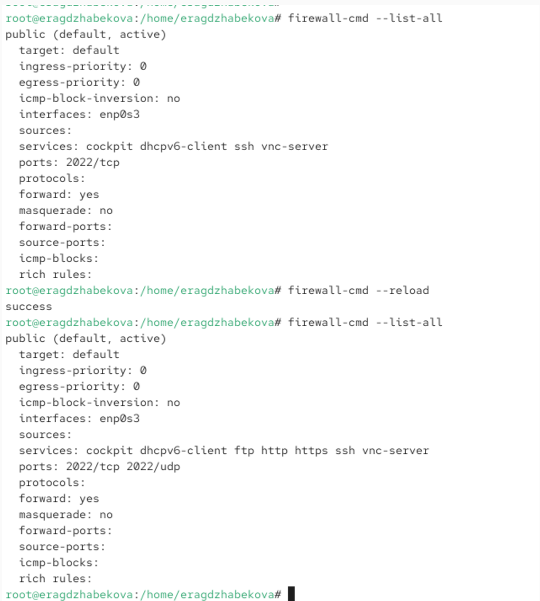
Add additional ports or port ranges, which need to be accessible for all hosts or networks that can connect to the machine.

Port	Protocol
2022	tcp
2022	udp

Connection to firewalld established. Changes applied.

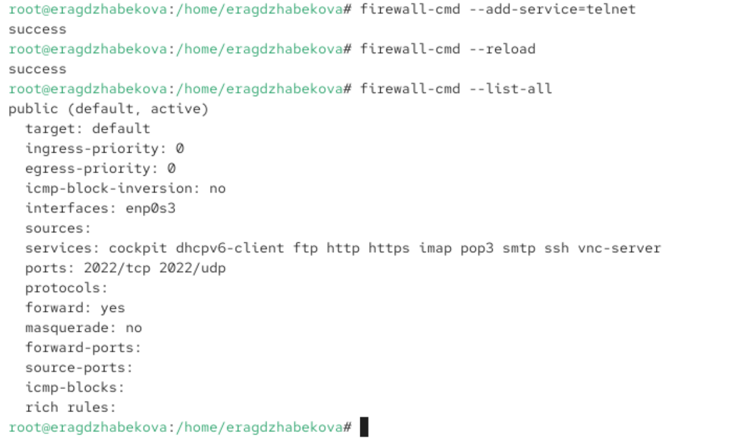
Default Zone: public **Log Denied:** off **Panic Mode:** disabled **Automatic Helpers:** no

Применение конфигурации



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

Добавление дополнительных служб



```
root@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --add-service=telnet
success
root@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --reload
success
root@eragdzhabekova:/home/eragdzhabekova# 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 vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@eragdzhabekova:/home/eragdzhabekova# 
```

Рис. 8: telnet, imap, pop3, smtp

Вывод

Вывод

В ходе работы освоены методы управления сетевыми правилами Linux с помощью **firewalld**:

- просмотр и анализ зон и сервисов,
- временное и постоянное добавление сервисов и портов,
- применение настроек через `firewall-cmd` и интерфейс `firewall-config`.

Получены практические навыки управления сетевой безопасностью и доступом.