

# Лабораторная работа №13

## Фильтр пакетов

---

Юсупова К. Р.

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Юсупова Ксения Равилевна
- Российский университет дружбы народов
- Номер студенческого билета- 1132247531
- [1132247531@pfur.ru]

## Вводная часть

---

## Цель работы

---

Получить навыки настройки пакетного фильтра в Linux.

## Выполнение лабораторной работы

---

# Выполнение лабораторной работы

Получили полномочия администратора, определили текущую зону по умолчанию, доступные зоны и посмотрели службы, доступные на компьютере

```
[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# firewall-cmd --get-default-zone
public
[root@yu ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@yu ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp
amqps apcupsd audit ausweisapp2 bacula bacula-client bareos-director bareos-fi
ledaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-tes
tnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent coc
kpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp
dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dro
pbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-prox
y freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp g
aleria ganglia-client ganglia-master git gpsd grafana gre high-availability htt
p http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target
isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell ku
be-api kube-apiserver kube-control-plane kube-control-plane-secure kube-contro
ller-manager kube-controller-manager-secure kube-nodeport-services kube-schedu
ler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker
ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp
llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt m
qtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs
nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storag
e console ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgre
sql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv p
tp pulseaudio puppetmaster quassel radius rdp redis sentinel rootd rpc-b
ind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip s
ips slp smtp smtp-submission smtps snmp snmp tls snmp trap snmptrap spidero
a lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing sync
thing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile3
8 tinc tor-socks transmission-client upnp-client vdsm vnc-server warpinator wb
em-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp
```

# Выполнение лабораторной работы

Определили доступные службы в текущей зоне и сравнили результаты вывода информации при использовании команды `firewall-cmd --list-all` и команды `firewall-cmd --list-all --zone=public`

```
[root@yu ~]# firewall-cmd --list-services
cockpit dhcpcv6-client ssh
[root@yu ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@yu ~]# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

## Выполнение лабораторной работы

Добавили сервер VNC в конфигурацию брандмауэра, проверили, что добавился vnc-server в конфигурацию. Перезапустили службу firewalld и проверили, что vnc-server нет в конфигурации, так как при использовании команды firewall-cmd –add-service=vnc-server без параметра –permanent правило добавляется только в текущую (runtime) конфигурацию брандмауэра, но не сохраняется в постоянную конфигурацию.

```
[root@yu ~]# firewall-cmd --add-service=vnc-server
success
[root@yu ~]# firewall-cmd --list-all
public (active)
    target: default
    icmp-block-inversion: no
    interfaces: enp0s3
    sources:
    services: cockpit dhcpcv6-client ssh vnc-server
    ports:
    protocols:
    forward: yes
    masquerade: no
    forward-ports:
    source-ports:
    icmp-blocks:
    rich rules:
[root@yu ~]# systemctl restart firewalld
[root@yu ~]# firewall-cmd --list-all
public (active)
    target: default
    icmp-block-inversion: no
    interfaces: enp0s3
    sources:
    services: cockpit dhcpcv6-client ssh
    ports:
    protocols:
    forward: yes
    masquerade: no
    forward-ports:
    source-ports:
    icmp-blocks:
```

## Выполнение лабораторной работы

Добавили службу vnc-server ещё раз, но на этот раз сделали её постоянной и проверили наличие vnc-server в конфигурации. Увидели, что VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения. Перезагрузите конфигурацию firewalld и просмотрели конфигурацию времени выполнения

```
[root@yu ~]# firewall-cmd --add-service=vnc-server --permanent
success
[root@yu ~]# firewall-cmd --list-all
public (active)
    target: default
    icmp-block-inversion: no
    interfaces: enp0s3
    sources:
    services: cockpit dhcpcv6-client ssh
    ports:
    protocols:
    forward: yes
    masquerade: no
    forward-ports:
    source-ports:
    icmp-blocks:
    rich rules:
[root@yu ~]# firewall-cmd --reload
success
[root@yu ~]# firewall-cmd --list-all
public (active)
    target: default
    icmp-block-inversion: no
    interfaces: enp0s3
    sources:
    services: cockpit dhcpcv6-client ssh vnc-server
    ports:
    protocols:
    forward: yes
    masquerade: no
    forward-ports:
    source-ports:
```

## Выполнение лабораторной работы

Добавили в конфигурацию межсетевого экрана порт 2022 протокола TCP и перезагрузили конфигурацию firewalld. Проверили, что порт добавлен в конфигурацию

```
[root@yu ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@yu ~]# firewall-cmd --reload
success
[root@yu ~]# firewall-cmd --list-all
public (active)
    target: default
    icmp-block-inversion: no
    interfaces: enp0s3
    sources:
    services: cockpit dhcpcv6-client ssh vnc-server
    ports: 2022/tcp
    protocols:
    forward: yes
    masquerade: no
    forward-ports:
    source-ports:
    icmp-blocks:
    rich rules:
```

Рис. 5: Выполнили пункты 14 и 15 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)

# Выполнение лабораторной работы

Открыли терминал и под учётной записью своего пользователя запустили интерфейс GUI `firewall-config`. Нажали выпадающее меню рядом с параметром `Configuration`. Открыли раскрывающийся список и выбрали `Permanent`. Это позволило сделать постоянными все изменения, которые вносим при конфигурировании. Выбирали зону `public` и отметили службы `http`, `https` и `ftp`, чтобы включить их.

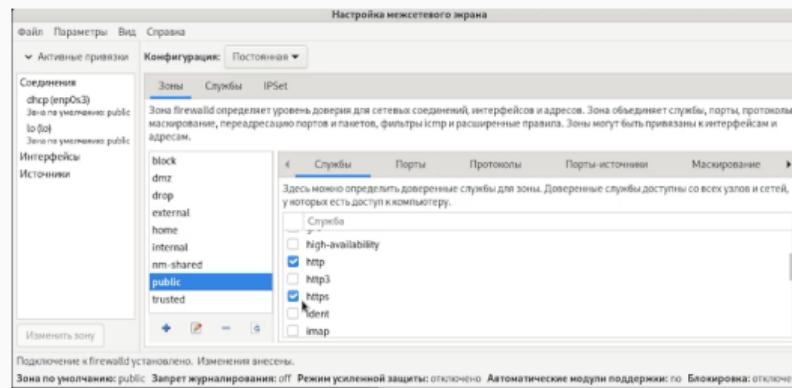


Рис. 6: Выполнили пункт 1-3 из раздела 13.4.2. (Управление брандмауэром с помощью `firewall-config`)

# Выполнение лабораторной работы

Выбрали вкладку Ports и на этой вкладке нажали Add . Ввели порт 2022 и протокол udp, закрыли утилиту firewall-config.

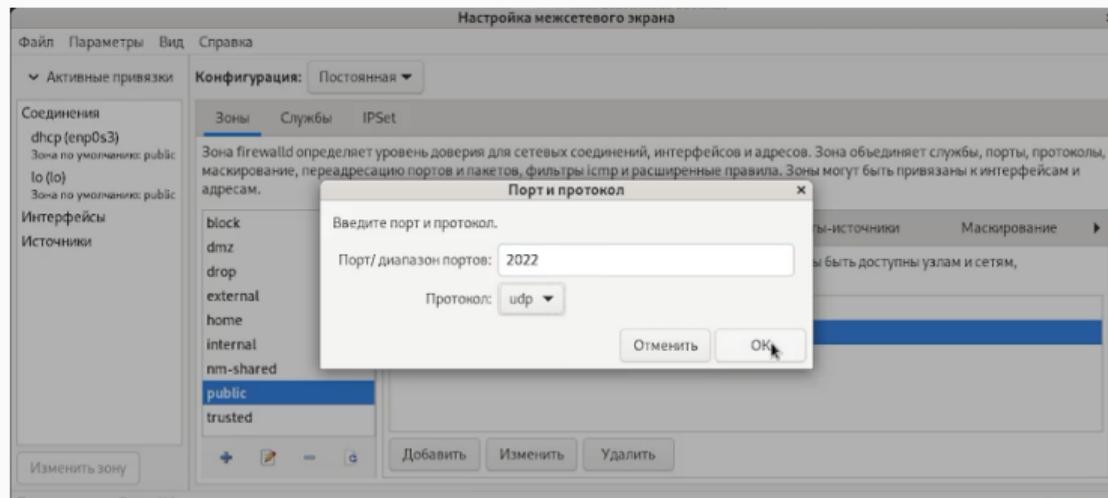


Рис. 7: Выполнили пункт 4 и 5 из раздела 13.4.2. (Управление брандмауэром с помощью firewall-config)

## Выполнение лабораторной работы

В окне терминала ввели firewall-cmd –list-all. Обратили внимание, что изменения, которые только что внесли, ещё не вступили в силу. Это связано с тем, что настроили их как постоянные изменения, а не как изменения времени выполнения. Перегрузили конфигурацию firewall-cmd и список доступных сервисов, увидели, что изменения были применены.

```
[ksyushadyu ~]$ firewall-config  
[ksyushadyu ~]$ firewall-cmd --list-all  
public (active)  
    target: default  
    icmp-block-inversion: no  
    interfaces: enp0s3  
    sources:  
    services: cockpit dhcpcv6-client ssh vnc-server  
    ports: 2022/tcp  
    protocols:  
    forward: yes  
    masquerade: no  
    forward-ports:  
    source-ports:  
    icmp-blocks:  
    rich rules:  
[ksyushadyu ~]$ firewall-cmd --reload  
success  
[ksyushadyu ~]$ firewall-cmd --list-all  
public (active)  
    target: default  
    icmp-block-inversion: no  
    interfaces: enp0s3  
    sources:  
    services: cockpit dhcpcv6-client ftp http https ssh vnc-server  
    ports: 2022/tcp 2022/udp  
    protocols:  
    forward: yes  
    masquerade: no  
    forward-ports:  
    source-ports:  
    icmp-blocks:
```

## Выполнение самостоятельной работы

---

## Выполнение самостоятельной работы

Создали в командной строке конфигурацию межсетевого экрана, которая позволяет получить доступ к службе telnet

```
[ksyusha@yu ~]$ firewall-cmd --add-service=telnet --permanent  
success  
[ksyusha@yu ~]$ █
```

Рис. 9: Выполнили пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)

# Выполнение самостоятельной работы

Создали в графическом интерфейсе конфигурацию межсетевого экрана, которая позволяет получить доступ для служб imap, pop3, smtp

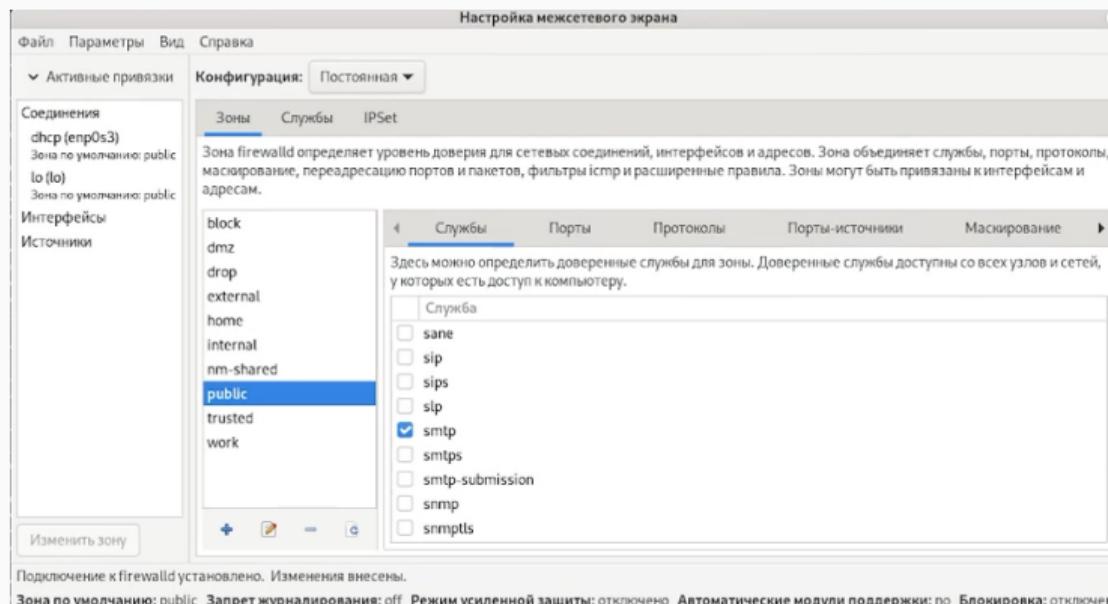


Рис. 10: Выполнili пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)

## Выполнение самостоятельной работы

Убедились, что конфигурация является постоянной и будет активирована после перезагрузки компьютера.

```
[ksyusha@yu ~]$ firewall-cmd --reload
success
[ksyusha@yu ~]$ firewall-cmd --list-all
public (active)
  target: default
  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:
[ksyusha@yu ~]$
```

Рис. 11: Выполнили пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)

## Выводы

---

## Выводы

---

В ходе лабораторной работы мы получили навыки настройки пакетного фильтра в Linux.