

# Фильтр пакетов

## Часть 1

---

Славинский В.В.

29 ноября 2025

Российский университет дружбы народов, Москва, Россия Россия

## Информация

---

..... {.columns align=center} ::: {.column width="70%"}

- Славинский Владислав Вадимович
- Студент
- Российский университет дружбы народов
- [1132246169@pfur.ru]

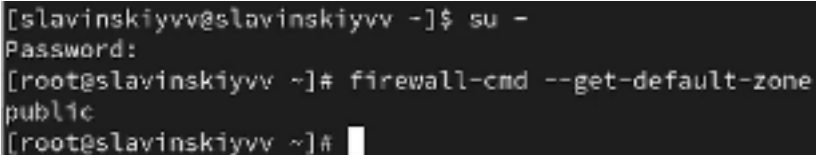
::: ::: {.column width="30%"}

## Вводная часть

---

## Определение текущей зоны по умолчанию

В терминале получим права администратора, определим текущую зону по умолчанию, введя:  
firewall-cmd --get-default-zone.

A terminal window with a dark background and light gray text. The prompt is [slavinskiyv@slavinskiyv ~]\$. The user enters 'su -'. The prompt changes to [root@slavinskiyv ~]#. The user enters 'firewall-cmd --get-default-zone'. The output is 'public'. The prompt returns to [root@slavinskiyv ~]#.

```
[slavinskiyv@slavinskiyv ~]$ su -  
Password:  
[root@slavinskiyv ~]# firewall-cmd --get-default-zone  
public  
[root@slavinskiyv ~]#
```

Рис. 1: sc1

Определим доступные зоны с помощью `firewall-cmd --get-zones`.

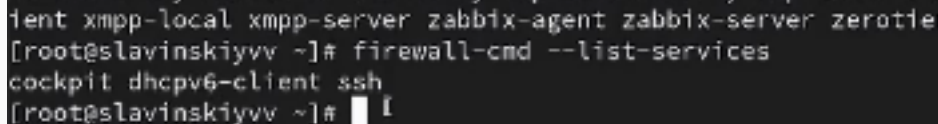
```
root@slavinskiyvv ~]# firewall-cmd --get-zones  
block dmz drop external home internal nm-shared public trusted work  
root@slavinskiyvv ~]#
```

Рис. 2: sc2

Посмотрим службы, доступные на компьютере, используя `firewall-cmd --get-services`.

```
[root@slavinskiyvv ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcups
d 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-ex
porter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds
dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registr
y docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman forema
n-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 iden
t imap imaps 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-plane k
ube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodep
ort-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kub
elet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp
llmnr-udp managiesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-w
bt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmap-0183 nrpe ntp
nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmp
roxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter
proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis se
ntinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane
slp slps slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lans
ync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui synthin
g-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-
client upnp-client vdsm vnc-server warpinator wbem-http wbem-https wireguard ws-discovery
ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-cl
ient xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
[root@slavinskiyvv ~]#
```

Определим доступные службы в текущей зоне: `firewall-cmd --list-services`.

A terminal window with a dark background and light gray text. The prompt is [root@slavinskiyvv ~]#. The command firewall-cmd --list-services has been executed, and the output lists several services: xmpp-local, xmpp-server, zabbix-agent, zabbix-server, zerotie, cockpit, dhcpv6-client, and ssh. The cursor is at the end of the last line.

```
ient xmpp-local xmpp-server zabbix-agent zabbix-server zerotie
[root@slavinskiyvv ~]# firewall-cmd --list-services
cockpit dhcpv6-client ssh
[root@slavinskiyvv ~]# █
```

Рис. 4: sc4



## Сравнение вывода информации

Сравним результаты вывода информации при использовании команды `firewall-cmd --list-all` и команды `firewall-cmd --list-all --zone=public`. Вывод у нас одинаковый, так как первая команда показывает текущую зону по умолчанию, по умолчанию у нас зона `public`, а вторая команда показывает конкретно зону `public`

```
cockpit dhcpv6-client ssh
[root@slavinskiyvv ~]# firewall-cmd --list-all
public (active)
  target: default
  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@slavinskiyvv ~]# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
```

Добавим сервер VNC в конфигурацию брандмауэра: `firewall-cmd --add-service=vnc-server`

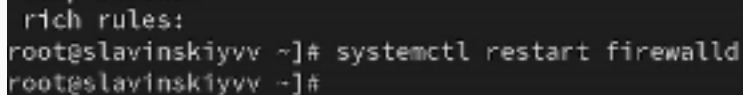
```
rich rules;  
[root@slavinskiyvv ~]# firewall-cmd --add-service=vnc-server  
success  
[root@slavinskiyvv ~]#
```

Рис. 6: sc6

Проверим, добавился ли vnc-server в конфигурацию: firewall-cmd --list-all.

```
[root@slavinskiyvv ~]# firewall-cmd --add-service=vnc-server
success
[root@slavinskiyvv ~]# firewall-cmd --list-all
public (active)
  target: default
  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:
```

Перезапустим службу firewalld: `systemctl restart firewalld`.

A terminal window with a dark background and light gray text. The text shows a user at a shell prompt entering the command to restart the firewalld service. The output of the command is visible on the first line.

```
rich rules:
root@slavinskiyvv ~]# systemctl restart firewalld
root@slavinskiyvv ~]#
```

Рис. 8: sc8

Проверим, есть ли vnc-server в конфигурации: `firewall-cmd --list-all`. vnc-server пропал, потому что служба была добавлена только во временную конфигурацию.

```
[root@slavinskiyvv ~]# systemctl restart firewalld
[root@slavinskiyvv ~]# firewall-cmd --list-all
public (active)
  target: default
  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:
```

Добавим службу vnc-server ещё раз, но на этот раз сделаем её постоянной, используя команду `firewall-cmd --add-service=vnc-server --permanent`.

```
tcp-blocks:  
rich rules:  
[root@slavinskiyvv ~]# firewall-cmd --add-service=vnc-server --permanent  
success  
[root@slavinskiyvv ~]#
```

Рис. 10: sc10

Проверим наличие vnc-server в конфигурации: firewall-cmd --list-all.

```
success
[root@slavinskiyvv ~]# firewall-cmd --list-all
public (active)
  target: default
  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@slavinskiyvv ~]#
```

## Перезагрузка конфигурации

Перезагрузим конфигурацию firewalld и посмотрим конфигурацию времени выполнения:  
firewall-cmd --reload, firewall-cmd --list-all.

```
source: port 22
icmp-blocks:
rich rules:
[root@slavinskiyv ~]# firewall-cmd --reload
success
[root@slavinskiyv ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
```



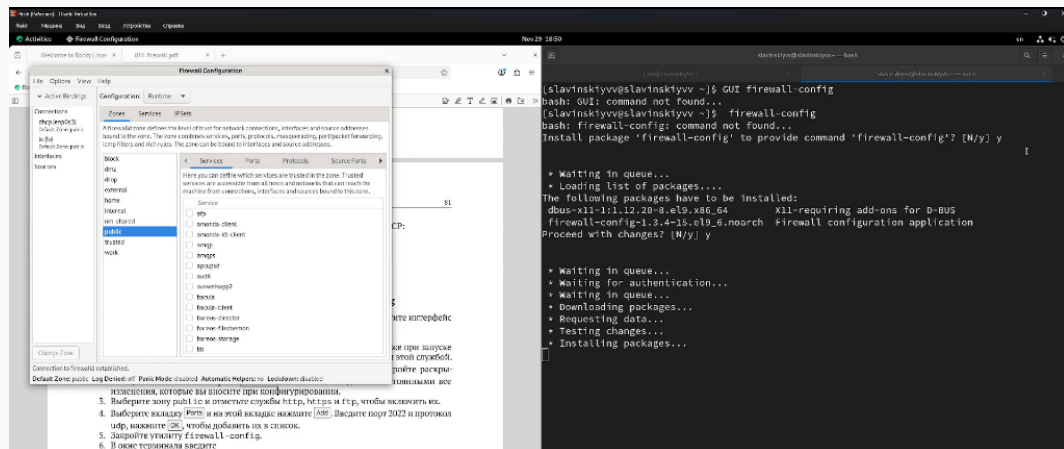
## Добавление порта

Добавим в конфигурацию межсетевого экрана порт 2022 протокола TCP: `firewall-cmd --add-port=2022/tcp --permanent`. Потом перезагрузим конфигурацию `firewalld` и проверим, что порт добавлен в конфигурацию.

```
firewall-cmd --add-port=2022/tcp --permanent
success
firewall-cmd --reload
success
firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
```

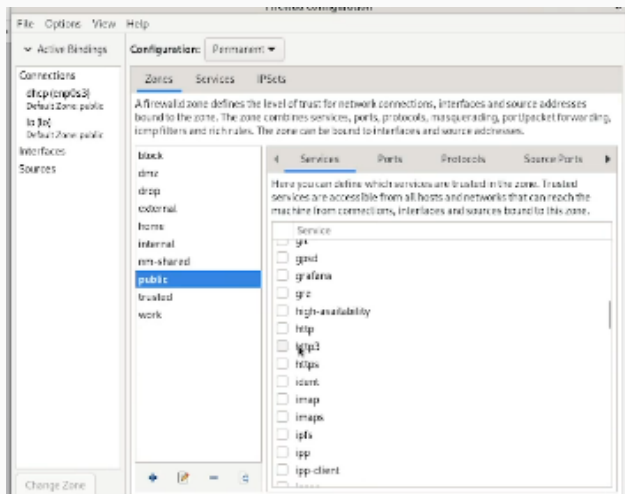
# Запуск интерфейса GUI

Откроем терминал и под учётной записью своего пользователя запустим интерфейс GUI  
firewall-config: firewall-config



## Изменение параметров

Далее в конфигурации выберем permanent. В зоне public выберем http ftp и https. Во вкладке ports введем 2022 и добавим протокол udr.



В окне терминала введем `firewall-cmd --list-all`

```
[slavinskiyvv@slavinskiyvv ~]$ firewall-cmd --list-all
public (active)
  target: default
  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:
[slavinskiyvv@slavinskiyvv ~]$
```

Перезагрузим конфигурацию firewalld: `firewall-cmd --reload`. И потом опять выведем список сервисов. Как видим, они добавились.

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

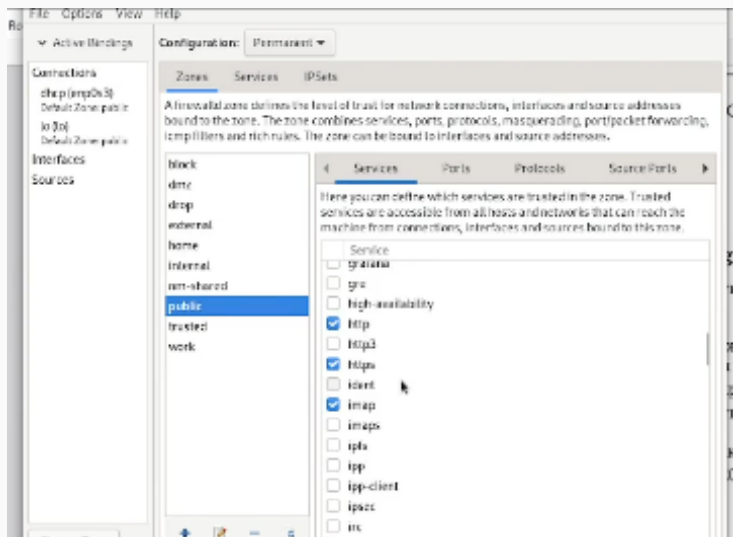
Создадим конфигурацию межсетевого экрана, которая позволяет получить доступ к службам telnet, imap, pop3, smtp. Через командную строку добавим telnet.

```
icmp=BLOCKS.  
rich rules:  
[slavinskiyvv@slavinskiyvv ~]$ firewall-cmd --add-service=telnet --permanent I
```

Рис. 18: sc18

## Добавление сервисов в графическом интерфейсе

Далее делаем в графическом интерфейсе GUI.



## Перезагрузка конфигурации и проверка

Перезагружаем конфигурацию firewalld и смотрим список доступных сервисов, как видим, все добавилось.

```
slavinskiyv@slavinskiyv -]$ firewall-cmd --add-service=telnet --permanent
success
slavinskiyv@slavinskiyv -]$ firewall-config
slavinskiyv@slavinskiyv -]$ firewall-cmd --reload
success
slavinskiyv@slavinskiyv -]$ 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:
```