

# Лабораторная работа №13

Фильтр пакетов

---

Комягин А.Н.

30 ноября 2024

Российский университет дружбы народов, Москва, Россия

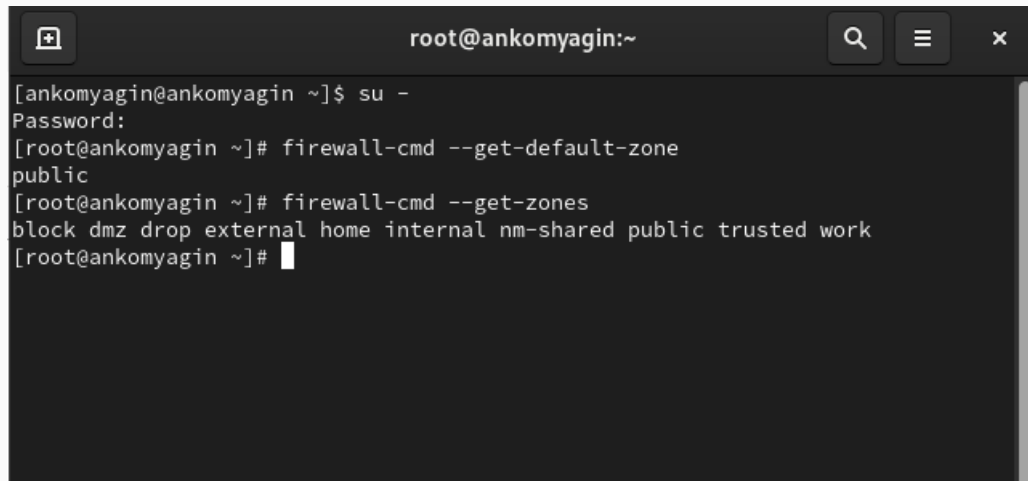
Цель

---

- Получить навыки настройки пакетного фильтра в Linux.

## Выполнение лабораторной работы

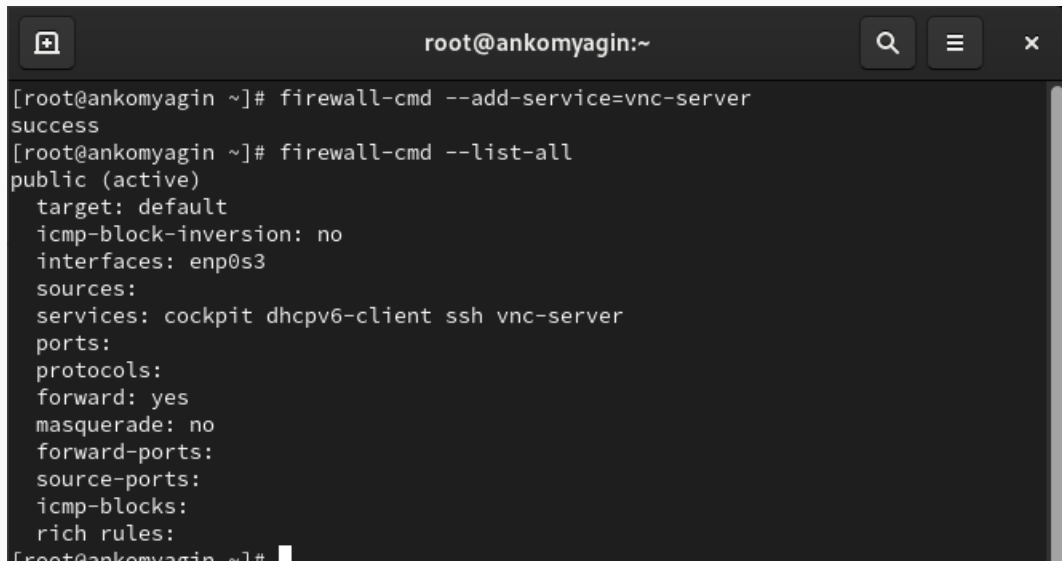
---

A terminal window with a dark background and light text. The title bar at the top shows 'root@ankomyagin:~' and has three icons on the right: a magnifying glass, a hamburger menu, and a close button. The terminal content shows a user switching to root and running two firewall commands. The first command returns 'public' as the default zone. The second command lists all available zones: 'block dmz drop external home internal nm-shared public trusted work'.

```
root@ankomyagin:~  
[ankomyagin@ankomyagin ~]$ su -  
Password:  
[root@ankomyagin ~]# firewall-cmd --get-default-zone  
public  
[root@ankomyagin ~]# firewall-cmd --get-zones  
block dmz drop external home internal nm-shared public trusted work  
[root@ankomyagin ~]#
```

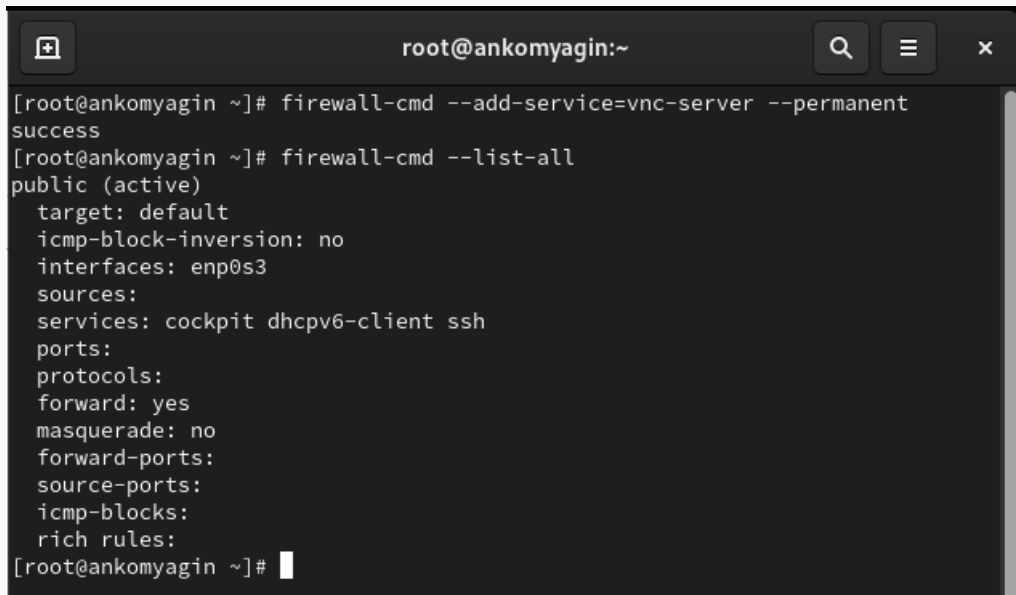
Рис. 1: Просмотр текущей зоны и доступных зон

## Добавление службы с конфигурацией Runtime



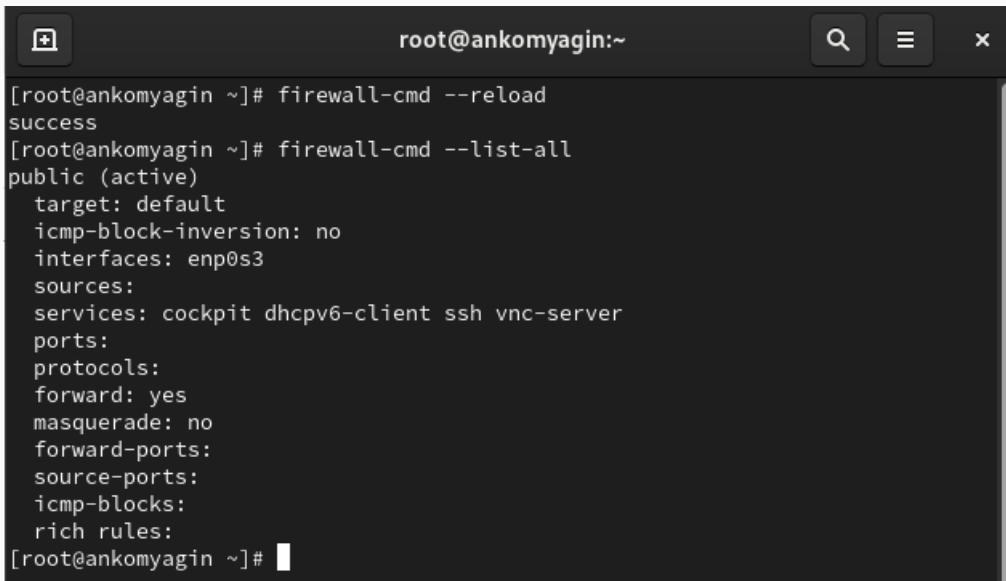
```
root@ankomyagin:~  
[root@ankomyagin ~]# firewall-cmd --add-service=vnc-server  
success  
[root@ankomyagin ~]# firewall-cmd --list-all  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: cockpit dhcpv6-client ssh vnc-server  
  ports: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

## Добавление службы с конфигурацией Permanent

A terminal window titled 'root@ankomyagin:~' with search, menu, and close icons in the top right. The terminal shows the execution of 'firewall-cmd --add-service=vnc-server --permanent' which returns 'success'. Then 'firewall-cmd --list-all' is run, displaying the current firewall configuration for the 'public' zone.

```
root@ankomyagin:~  
[root@ankomyagin ~]# firewall-cmd --add-service=vnc-server --permanent  
success  
[root@ankomyagin ~]# 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@ankomyagin ~]#
```

## Добавление службы с конфигурацией Permanent

A terminal window titled 'root@ankomyagin:~' with search, menu, and close icons in the top right. The terminal shows the execution of 'firewall-cmd --reload' which returns 'success', followed by 'firewall-cmd --list-all' which displays the current firewall configuration for the 'public' zone.

```
[root@ankomyagin ~]# firewall-cmd --reload
success
[root@ankomyagin ~]# 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:
[root@ankomyagin ~]#
```



# Работа через графический интерфейс

The image shows a terminal window and a graphical user interface for firewall configuration. The terminal window at the top shows a user logging out and running the `firewall-config` command. Below the terminal is the **Firewall Configuration** GUI. The GUI has a sidebar with sections: **Active Bindings**, **Connections** (showing `lo (lo)` and `dhcp (enp0s3)`), **Interfaces**, and **Sources**. The **Configuration:** dropdown is set to **Runtime**. The main panel has tabs for **Zones**, **Services**, and **IPSets**. The **Zones** tab is active, showing a description of a firewall zone and a list of zones: `block`, `dmz`, `drop`, `external`, `home`, `internal`, `nm-shared`, **`public`** (selected), `trusted`, and `work`. The **Services** tab is also visible, showing a list of services with checkboxes: `afp`, `amanda-client`, `amanda-k5-client`, `amqp`, `amqps`, `apcupsd`, `audit`, `ausweisapp2`, `bacula`, and `bash`.

Terminal output:

```
ankomyagin@ankomyagin:~ — bash
[root@ankomyagin ~]# exit
logout
[ankomyagin@ankomyagin ~]$ firewall-config
```

Firewall Configuration GUI:

- Configuration:** Runtime
- Zones:** A firewall 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.
- Services:** 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
<input type="checkbox"/> afp
<input type="checkbox"/> amanda-client
<input type="checkbox"/> amanda-k5-client
<input type="checkbox"/> amqp
<input type="checkbox"/> amqps
<input type="checkbox"/> apcupsd
<input type="checkbox"/> audit
<input type="checkbox"/> ausweisapp2
<input type="checkbox"/> bacula
<input type="checkbox"/> bash

## Ответы на контрольные вопросы

---

## 1. Какая служба должна быть запущена перед началом работы с менеджером конфигурации брандмауэра firewall-config?

Нужно запустить службу firewalld, это можно сделать командой `systemctl start firewalld`.

2. Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию?

Команда `firewall-cmd --add-port=2355/udp --permanent`.

### 3. Какая команда позволяет показать всю конфигурацию брандмауэра во всех зонах?

Команда `firewall-cmd --list-all-zones`.

4. Какая команда позволяет удалить службу vnc-server из текущей конфигурации брандмауэра?

Команда `firewall-cmd --remove-service=vnc-server --permanent`.

5. Какая команда `firewall-cmd` позволяет активировать новую конфигурацию, добавленную опцией `–permanent`?

Команда `firewall-cmd –reload`.

6. Какой параметр `firewall-cmd` позволяет проверить, что новая конфигурация была добавлена в текущую зону и теперь активна?

Команда `firewall-cmd --list-all`.



## 7. Какая команда позволяет добавить интерфейс eno1 в зону public?

Команда `firewall-cmd --zone=public --add-interface=eno1 --permanent`.

8. Если добавить новый интерфейс в конфигурацию брандмауэра, пока не указана зона, в какую зону он будет добавлен?

Он будет добавлен в зону по умолчанию.

## Вывод

---

Я получил навыки настройки пакетного фильтра в Linux.