

# **Отчёт по лабораторной работе №13**

## **Фильтр пакетов**

Борисенкова София Павловна

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение лабораторной работы</b>	<b>6</b>
<b>3 Контрольные вопросы</b>	<b>12</b>
<b>4 Заключение</b>	<b>13</b>

# **Список иллюстраций**

2.1	Определение зоны и служб . . . . .	6
2.2	Просмотр конфигурации зоны . . . . .	7
2.3	Добавление vnc-server . . . . .	8
2.4	Добавление порта 2022/tcp . . . . .	8
2.5	Настройка служб в firewall-config . . . . .	9
2.6	Применение настроек firewall-config . . . . .	9

# **Список таблиц**

# **1 Цель работы**

Получить навыки настройки пакетного фильтра в Linux.

## **2 Выполнение лабораторной работы**

Получаю привилегии администратора, определяю зону по умолчанию и просматриваю доступные зоны (см. рис. fig. 2.1).

Рис. 2.1: Определение зоны и служб

Определяю службы, доступные в текущей зоне. Сравниваю вывод команд `firewall-cmd --list-all` и `firewall-cmd --list-all --zone=public` (см. рис. fig. 2.2).



```
root@localhost:~--bash
root@localhost:~--bash
root@localhost:~# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@localhost:~# 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@localhost:~# 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@localhost:~#
```

Рис. 2.2: Просмотр конфигурации зоны

Добавляю службу vnc-server в конфигурацию брандмауэра и проверяю, что служба добавлена: (см. рис. fig. 2.3).

Перезапускаю службу firewalld командой systemctl restart firewalld, затем снова просматриваю конфигурацию — служба vnc-server исчезает, поскольку ранее была добавлена только во время выполнения

Добавляю службу vnc-server на постоянной основе командой firewall-cmd --add-service=vnc-server --permanent. Проверяю конфигурацию — служба не отображается, так как изменения постоянной конфигурации не активируются автоматически

Перезагружаю конфигурацию firewall-cmd --reload и снова просматриваю параметры зоны — служба vnc-server появляется

```

root@localhost:~# firewall-cmd --add-service=vnc-server
success
root@localhost:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@localhost:~# systemctl restart firewalld
root@localhost:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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:

```

Рис. 2.3: Добавление vnc-server

Добавляю порт 2022/tcp в постоянную конфигурацию и после перезагрузки убеждаюсь, что порт добавлен (см. рис. fig. 2.4).

```

root@localhost:~# firewall-cmd --add-service=vnc-server --permanent
success
root@localhost:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@localhost:~# firewall-cmd --reload
success
root@localhost:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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:

```

Рис. 2.4: Добавление порта 2022/tcp

Запускаю графическую утилиту firewall-config (см. рис. fig. ??).

В меню Configuration выбираю Permanent.

Перехожу в зону public и включаю службы http, https и ftp (см. рис. fig. 2.5).

```

root@localhost:~# firewall-cmd --add-port=2022/tcp --permanent
success
root@localhost:~# firewall-cmd --reload
success
root@localhost:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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:
root@localhost:~# 

```

Рис. 2.5: Настройка служб в firewall-config

На вкладке Ports нажимаю Add и добавляю порт 2022/udp

Проверяю конфигурацию `firewall-cmd --list-all` — изменения не вступили в силу, так как были добавлены только в постоянный профиль.

Перезагружаю конфигурацию `firewall-cmd --reload` и снова просматриваю настройки — изменения применены (см. рис. fig. 2.4).

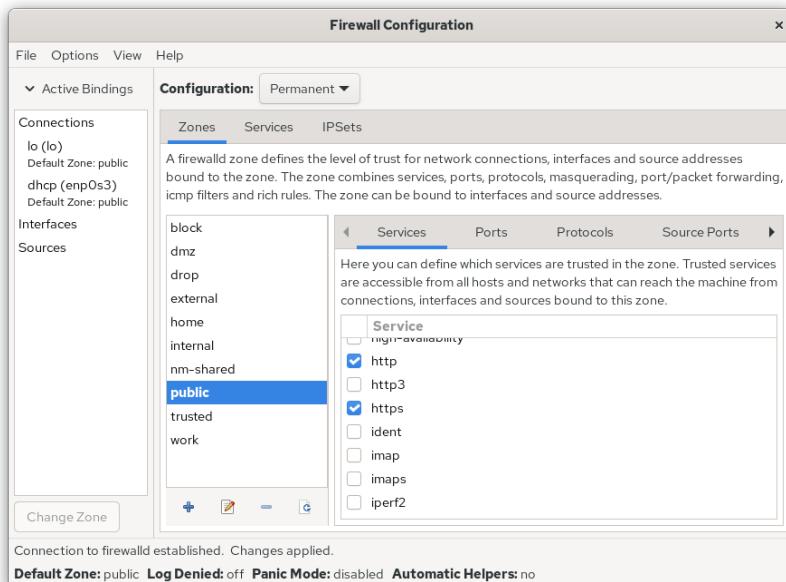
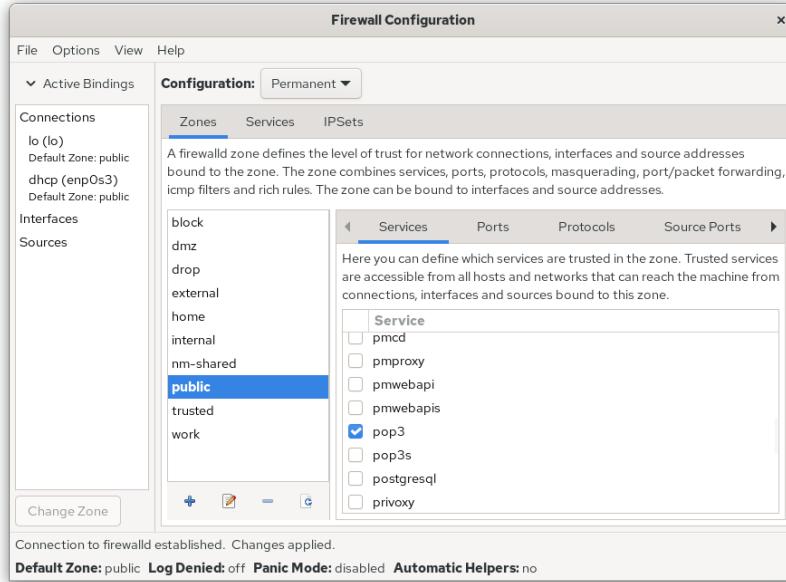
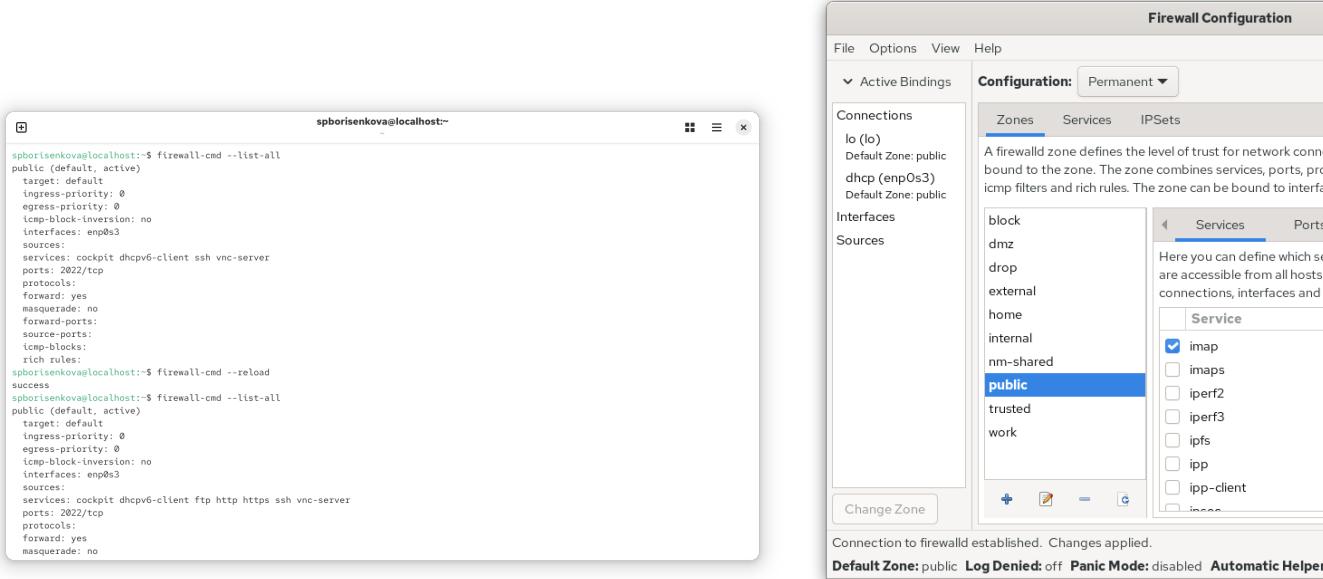


Рис. 2.6: Применение настроек firewall-config

Создаю конфигурацию межсетевого экрана, позволяющую доступ к службам **telnet**, **imap**, **pop3** и **smtp**.

Открываю утилиту **firewall-config** и перехожу в режим **Permanent**.

Выбираю зону **public** и отмечаю службы **imap**, **pop3** и **smtp** в списке (см. рис. fig. ??).



Добавляю службу **telnet** через командную строку, используя постоянное добавление, чтобы правило сохранилось на диске и применялось после перезагрузки

После внесения изменений проверяю конфигурацию в терминале.

Службы **telnet**, **imap**, **pop3** и **smtp** присутствуют в списке и отмечены как активные и постоянные, что подтверждает корректное применение настроек после перезагрузки системы

### **3 Контрольные вопросы**

1. Должна быть запущена служба firewalld.
2. firewall-cmd –add-port=2355/udp –permanent
3. firewall-cmd –list-all-zones
4. firewall-cmd –remove-service=vnc-server
5. firewall-cmd –reload
6. firewall-cmd –list-all
7. firewall-cmd –zone=public –add-interface=en01 –permanent
8. В зону по умолчанию

## **4 Заключение**

В ходе лабораторной работы были освоены приёмы управления брандмауэром в Linux