# Отчёт по лабораторной работе №13

**Фильтр пакетов**

Тукаев Тимур

# Содержание

# Список иллюстраций

# Список таблиц

# 1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

# 2 Выполнение

## 2.1 Управление брандмауэром с помощью firewall-cmd

1. Получены права суперпользователя с помощью команды `su -`.
   После ввода пароля выполнен переход в контекст root.


Рис. 2.1: Получение прав root

2. Определена текущая зона брандмауэра (`firewall-cmd --get-default-zone`).
   Используется зона **public**.

3. Просмотрены все доступные зоны (`firewall-cmd --get-zones`).
   Выведен список предустановленных зон.

4. Получен перечень всех поддерживаемых служб (`firewall-cmd --get-services`).
   Выведен длинный список доступных сервисов.

5. Определены разрешённые в текущей зоне службы (`firewall-cmd --list-services`).

В зоне **public** активны: `cockpit`, `dhcpv6-client`, `ssh`.

6. Выполнено сравнение вывода команд `firewall-cmd --list-all` и `firewall-cmd --list-all --zone=public`.
   Результаты совпадают, подтверждая, что активной зоной по умолчанию является **public**.


Рис. 2.2: Просмотр конфигурации зоны

7. Добавлена служба **vnc-server** во временную конфигурацию (`firewall-cmd --add-service=vnc-server`).

8. Повторная проверка (`firewall-cmd --list-all`).
   Служба **vnc-server** появилась в зоне.

9. Перезапущена служба firewalld (`systemctl restart firewalld`).

10. После проверки (`firewall-cmd --list-all`) служба **vnc-server** исчезла.
    Причина: добавление было сделано только во время выполнения (runtime), а не сохранено на диск.

```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# firewall-cmd --add-service=vnc-server
success
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev# systemctl restart firewalld.service
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev#
```

Рис. 2.3: Добавление VNC

11. Служба VNC добавлена **постоянно** (`firewall-cmd --add-service=vnc-server --permanent`).

12. Проверка (`firewall-cmd --list-all`) показала отсутствие изменений в runtime.
    Постоянные настройки не применяются автоматически.

13. Загружена постоянная конфигурация и выполнена проверка (`firewall-cmd --reload`, затем `firewall-cmd --list-all`).

    Служба **vnc-server** снова присутствует.

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

Рис. 2.4: Применение конфигурации

14. В постоянную конфигурацию добавлен порт **2022/tcp** (`firewall-cmd --add-port=2022/tcp --permanent`).

    После загрузки конфигурации (`firewall-cmd --reload`) порт отображается в списке активных.

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

Рис. 2.5: Добавление порта 2022/tcp

## 2.2 Управление брандмауэром с помощью firewall-config

1. Запущено приложение `firewall-config`.
   При запуске потребовалось подтверждение прав администратора.

2. В интерфейсе выбрана конфигурация **Permanent**, чтобы изменения сохранялись на диске.

3. В зоне **public** активированы службы `http`, `https`, `ftp`.

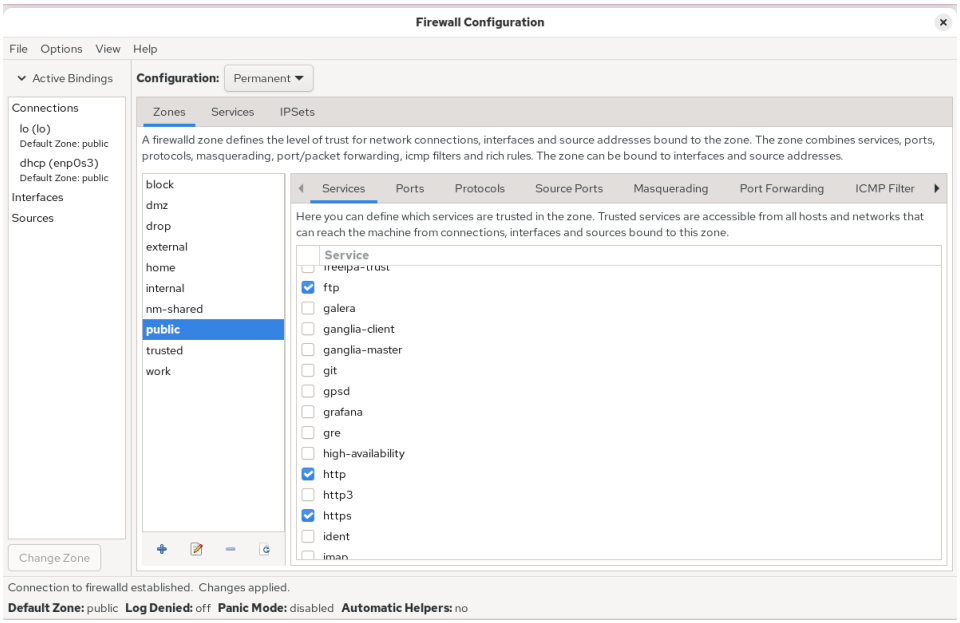


Рис. 2.6: GUI firewall-config: включение служб

4. На вкладке *Ports* добавлен порт **2022** с протоколом UDP.

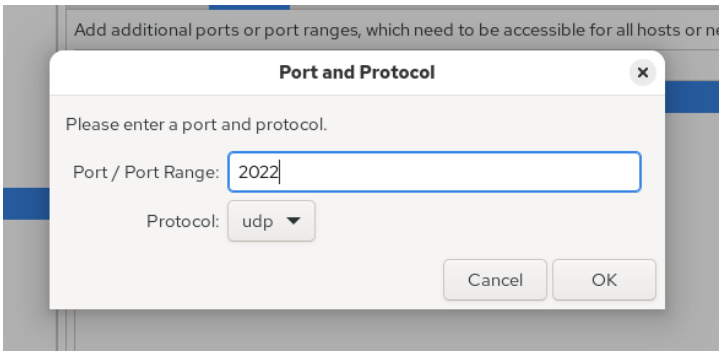


Рис. 2.7: Добавление порта UDP

5. Утилита закрыта, затем снова проверена текущая конфигурация (`firewall-cmd --list-all`).
   Изменения ещё не отображаются (внесены как permanent).

6. Загружена конфигурация (`firewall-cmd --reload`).
   После повторной проверки изменения применены: службы и порты отображаются в списке.

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

Рис. 2.8: Изменения вступили в силу

## 2.3 Самостоятельная работа

Выполнена конфигурация доступа к службам:

- telnet — добавлена через командную строку (постоянно)
- imap, pop3, smtp — включены через `firewall-config`

После загрузки конфигурации все службы присутствуют в списке.

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

Рис. 2.9: Конечная конфигурация с telnet, imap, pop3, smtp

# 3 Контрольные вопросы

1. Перед началом работы с менеджером конфигурации брандмауэра **firewall-config** должна быть запущена служба `firewalld`.
2. Добавление порта **2355/udp** в конфигурацию брандмауэра выполняется командой
   `firewall-cmd --add-port=2355/udp`.
3. Для отображения полной конфигурации брандмауэра во всех зонах используется команда
   `firewall-cmd --list-all-zones`.
4. Удаление службы **vnc-server** из текущей конфигурации выполняется командой
   `firewall-cmd --remove-service=vnc-server`.
5. Активация новой конфигурации, сохранённой через опцию `--permanent`, происходит после выполнения команды
   `firewall-cmd --reload`.
6. Проверить, что новая конфигурация применена и активна, можно командой `firewall-cmd --list-all`.
7. Добавление интерфейса **eno1** в зону `public` выполняется командой
   `firewall-cmd --zone=public --change-interface=eno1`.
8. Если зона не указана при добавлении нового интерфейса, он будет автоматически добавлен в **зону по умолчанию** (default zone).

# 4 Заключение

В ходе лабораторной работы были изучены способы настройки межсетевого экрана с использованием инструментов `firewall-cmd` и `firewall-config`.
Были рассмотрены различия между временной (runtime) и постоянной (permanent) конфигурациями, а также порядок применения изменений.
На практике выполнены операции по добавлению и удалению служб и портов, назначению интерфейсов зонам и обновлению конфигурации брандмауэра.