Отчёт по лабораторной работе №13

Дисциплина: Основы администрирования операционных систем

Верниковская Екатерина Андреевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2 Задание

1. Используя firewall-cmd:

- определить текущую зону по умолчанию
- определить доступные для настройки зоны
- определить службы, включённые в текущую зону
- добавить сервер VNC в конфигурацию брандмауэра

2. Используя firewall-config:

- добавить службы http и ssh в зону public
- добавить порт 2022 протокола UDP в зону public
- добавить службу ftp

3. Выполнить задание для самостоятельной работы

3 Выполнение лабораторной работы

3.1 Управление брандмауэром с помощью firewall-cmd

Запускаем терминала и получаем полномочия суперпользователя, используя *su* - (рис. 3.1)

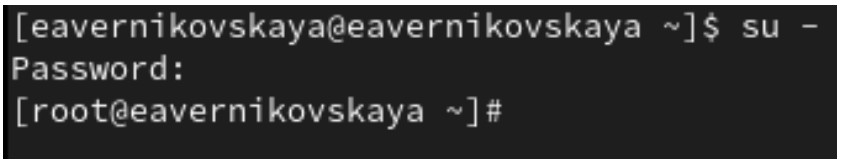

Рис. 3.1: Режим суперпользователя

Определим текущую зону по умолчанию, введя: *firewall-cmd –get-default-zone* (рис. 3.2)

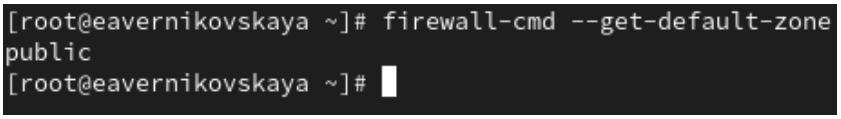

Рис. 3.2: Определение текущей зоны по умолчанию

Определим доступные зоны, введя: *firewall-cmd –get-zones* (рис. 3.3)

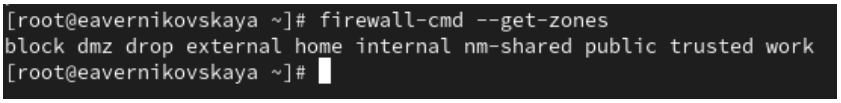

Рис. 3.3: Определение доступных зон

Посмотрим службы, доступные на нашем компьютере, используя *firewall-cmd –get-services* (рис. 3.4)

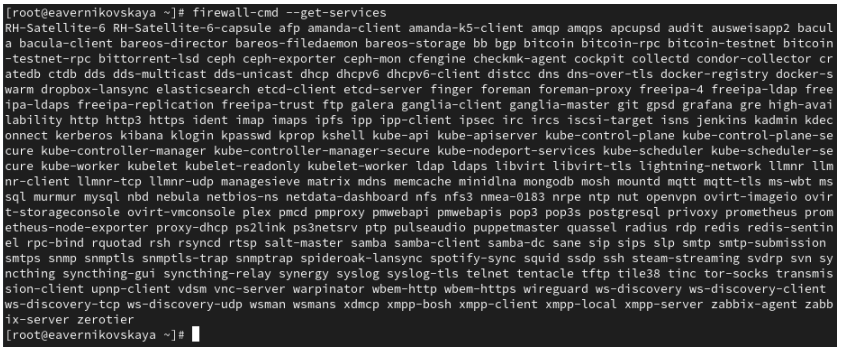

Рис. 3.4: Службы доступные на нашем компьютере

Определим доступные службы в текущей зоне: *firewall-cmd –list-services* (рис. 3.5)

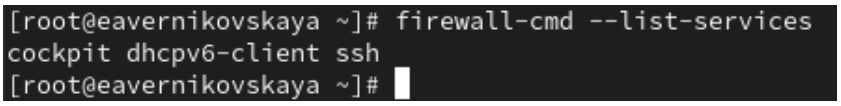

Рис. 3.5: Определение доступных служб в текущей зоне

Сравним результаты вывода информации при использованиии команд *firewall-cmd –list-all* и *firewall-cmd –list-all –zone=public*. Результат одинаковый, так как в настоящее время зона public является активной зоной по умолчанию (рис. 3.6), (рис. 3.7)

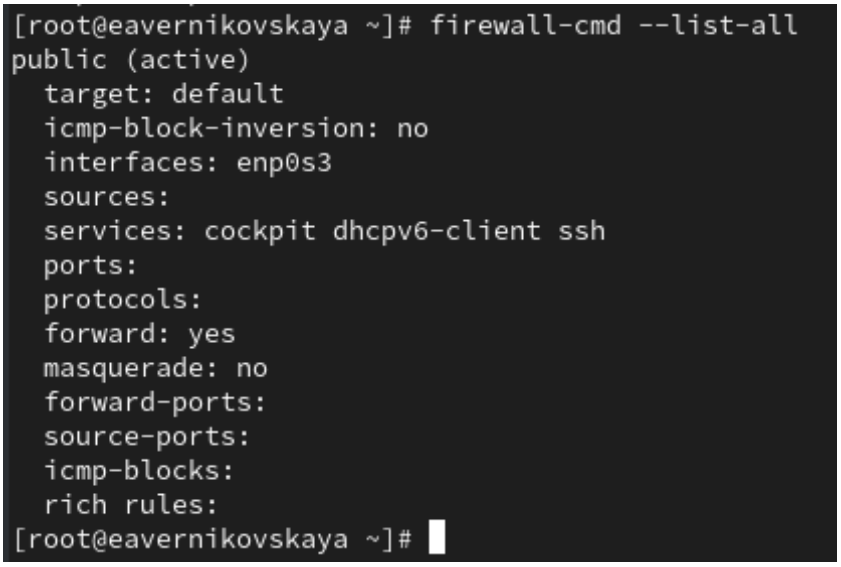

Рис. 3.6: Вывод команды firewall-cmd –list-all

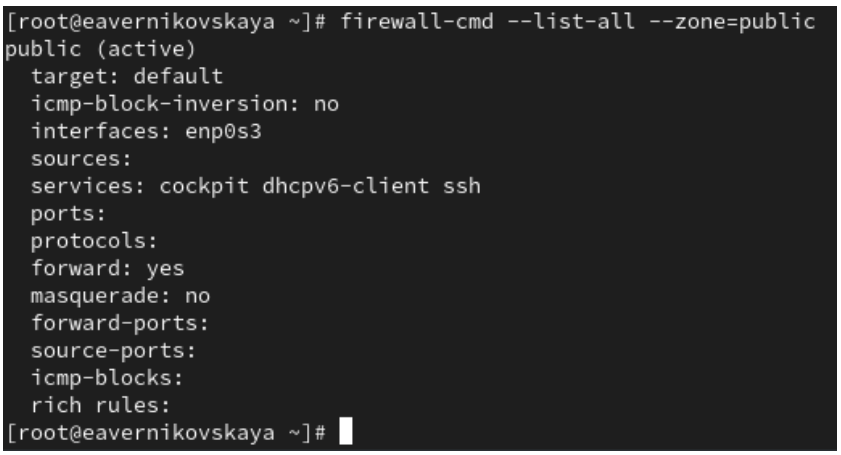

Рис. 3.7: Вывод команды firewall-cmd –list-all –zone=public

Добавим сервер VNC в конфигурацию брандмауэра: *firewall-cmd –add-service=vnc-server* (рис. 3.8)

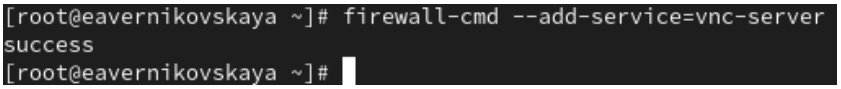

Рис. 3.8: Добавление сервера VNC в конфигурацию брандмауэра

Проверим, добавился ли vnc-server в конфигурацию: *firewall-cmd –list-all* (рис. 3.9)

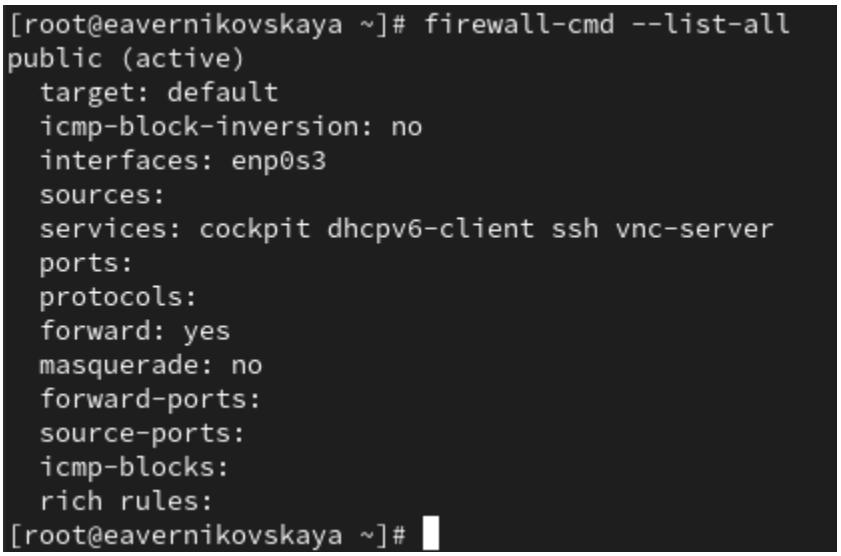

Рис. 3.9: Проверка добавления сервера VNC в конфигурацию

Перезапустим службу firewalld: *systemctl restart firewalld* (рис. 3.10)

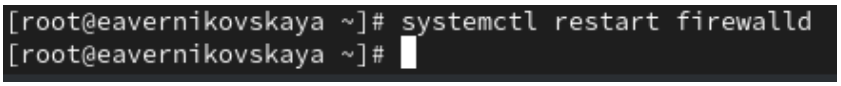

Рис. 3.10: Перезапуск службы firewalld

Проверим, есть ли vnc-server в конфигурации: *firewall-cmd –list-all*. Его нет, так как служба vnc-server не постоянная (рис. 3.11)

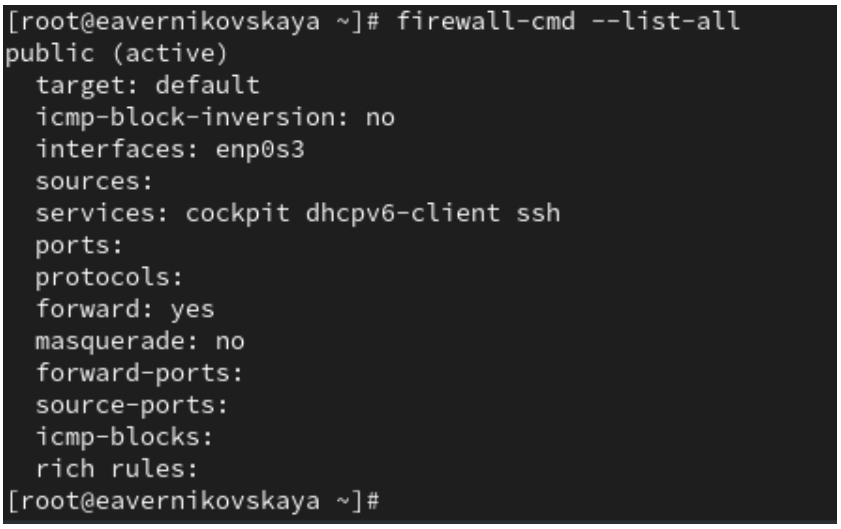

Рис. 3.11: Проверка наличия сервера VNC в конфигурации после перезапуска

Добавим службу vnc-server ещё раз, но на этот раз сделаем её постоянной, используя команду *firewall-cmd –add-service=vnc-server –permanent* (рис. 3.12)

Рис. 3.12: Добавление постоянного сервера VNC в конфигурацию брандмауэра

Проверим наличие vnc-server в конфигурации: *firewall-cmd –list-all*. Мы увидим, что VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения (рис. 3.13)

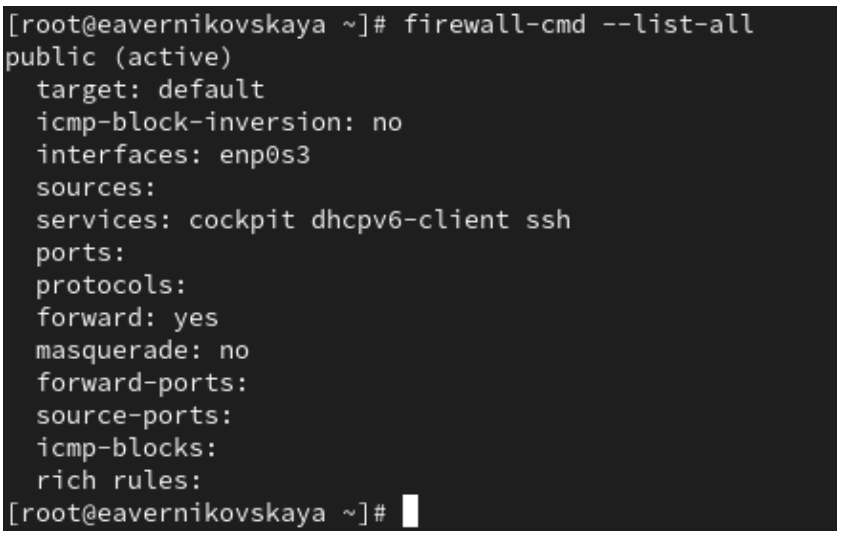

Рис. 3.13: Проверка наличия постоянного сервера VNC в конфигурации

Перезагрузим конфигурацию firewalld и посмотрим конфигурацию времени выполнения: *firewall-cmd –reload* и *firewall-cmd –list-all* (рис. 3.14), (рис. 3.15)

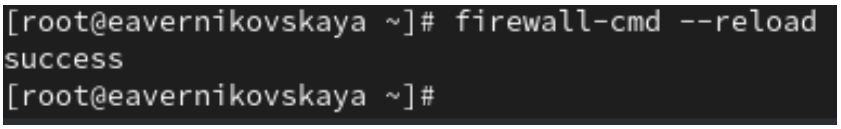

Рис. 3.14: Перезагрузка конфигурации firewalld (1)

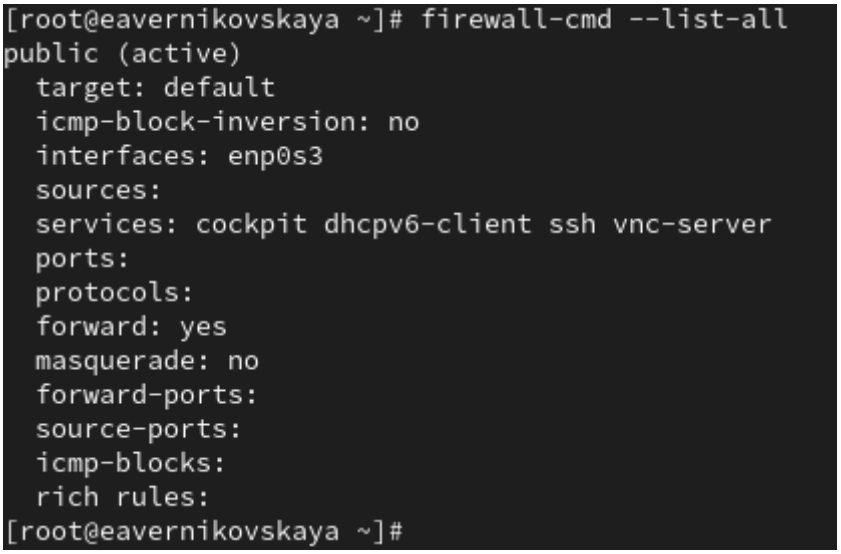

Рис. 3.15: Просмотр конфигурации времени выполнения

Добавим в конфигурацию межсетевого экрана порт 2022 протокола TCP: *firewall-cmd –add-port=2022/tcp –permanent* (рис. 3.16)

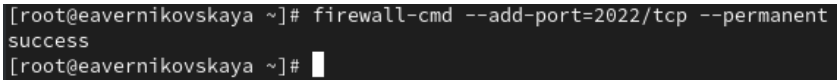

Рис. 3.16: Добавление порта в конфигурацию

Затем снова перезагрузим конфигурацию firewalld: *firewall-cmd –reload* (рис. 3.17)

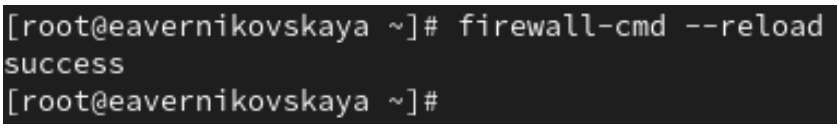

Рис. 3.17: Перезагрузка конфигурации firewalld (2)

И проверим, что порт добавлен в конфигурацию: *firewall-cmd –list-all* (рис. 3.18)

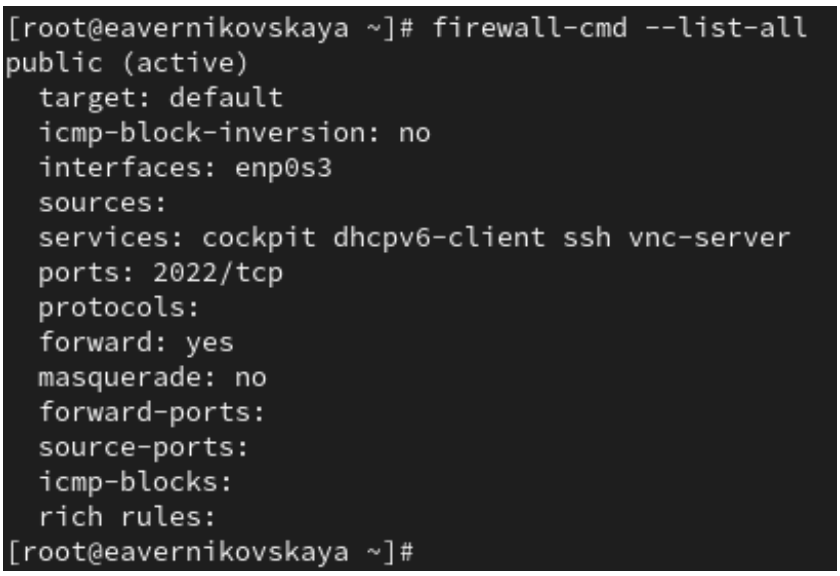

Рис. 3.18: Проверка добавления порта в конфигурацию

3.2 Управление брандмауэром с помощью firewall-config

Открываем терминал и под учётной записью нашего пользователя запускаем интерфейс GUI firewall-config: *firewall-config*. Служба отсутствует, и система

предлагает нам её установить. Также при запуске вводим пароль пользователя с полномочиями управления этой службой (рис. 3.19), (рис. 3.20), (рис. 3.21)

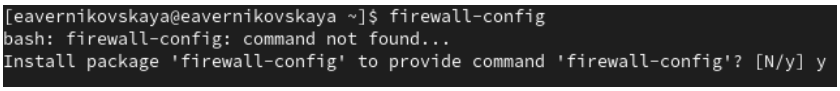

Рис. 3.19: Установка firewall-config

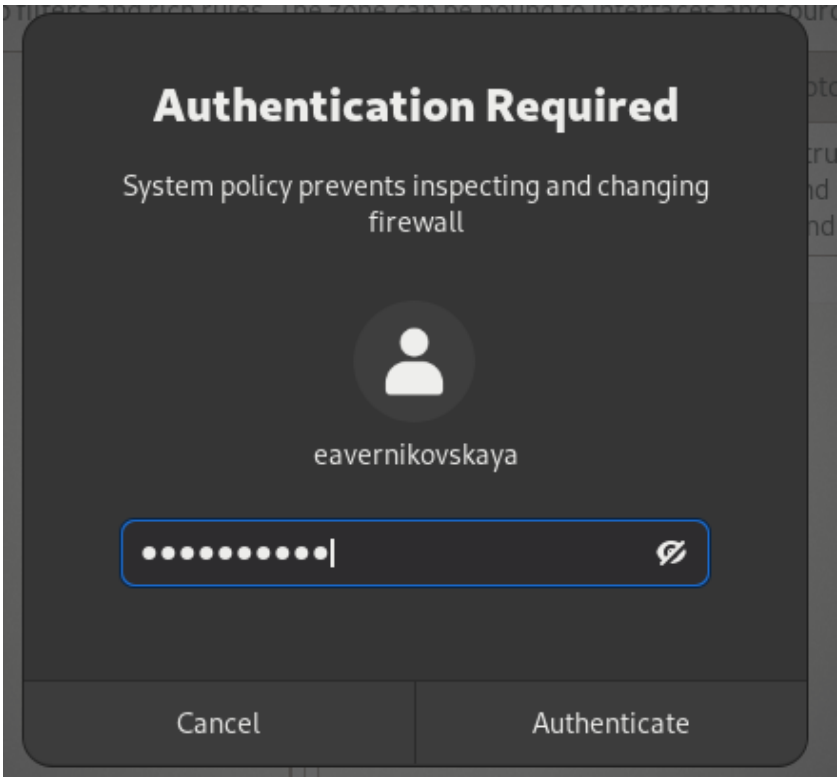

Рис. 3.20: Ввод пароля

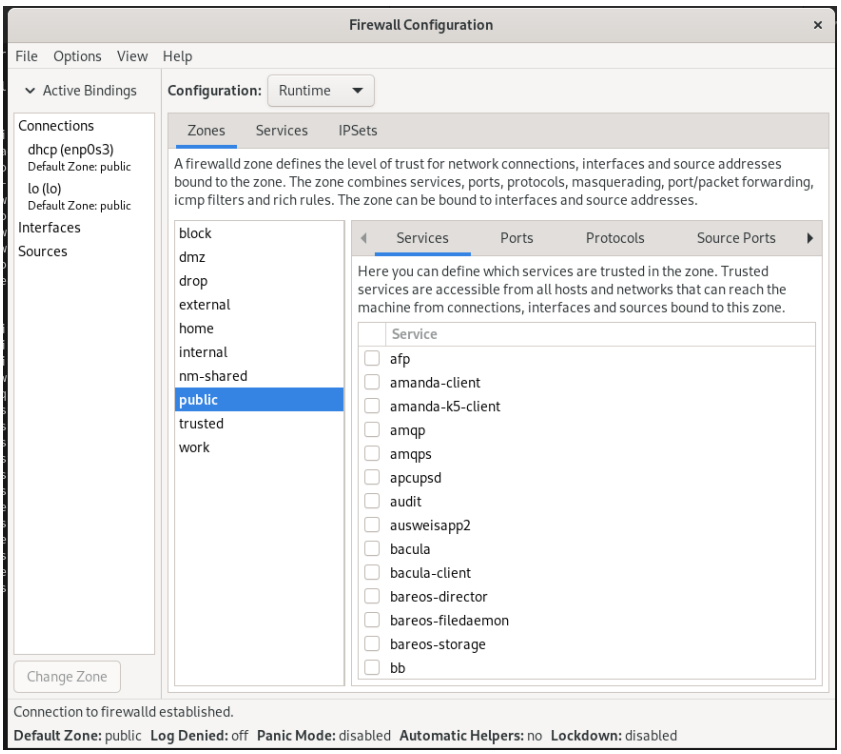

Рис. 3.21: Интерфейс GUI firewall-config

Нажимаем выпадающее меню рядом с параметром Configuration. Открываем раскрывающийся список и выбираем Permanent. Это позволит сделать постоянными все изменения, которые мы вносим при конфигурировании (рис. 3.22)

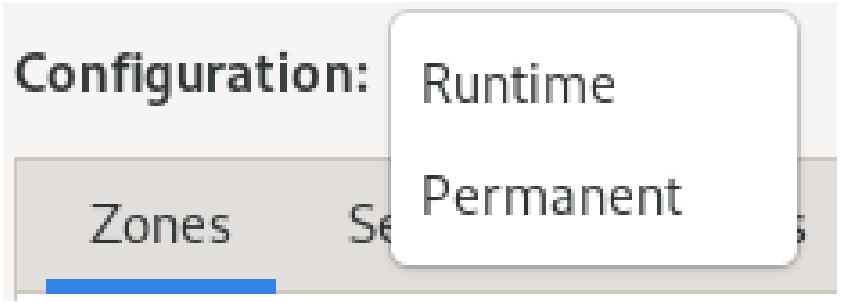

Рис. 3.22: Выбор Permanent

Выбираем зону public и отмечаем службы http, https и ftp, чтобы включить их (рис. 3.23)

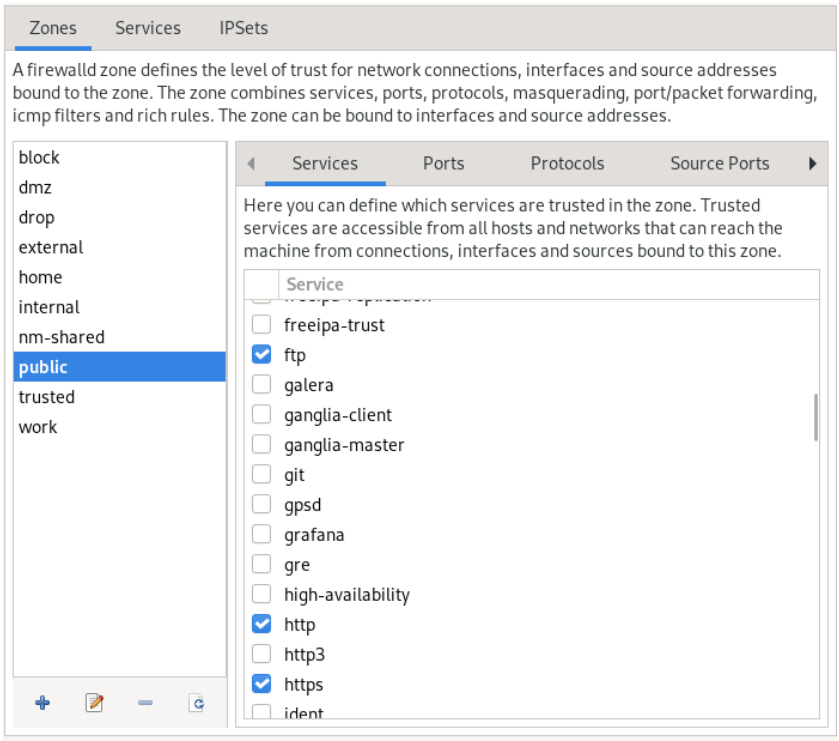

Рис. 3.23: Включение служб http, https и ftp

Выбираем вкладку Ports и на этой вкладке нажимаем Add. Вводим порт 2022 и протокол udp, нажимаем OK, чтобы добавить их в список (рис. 3.24)

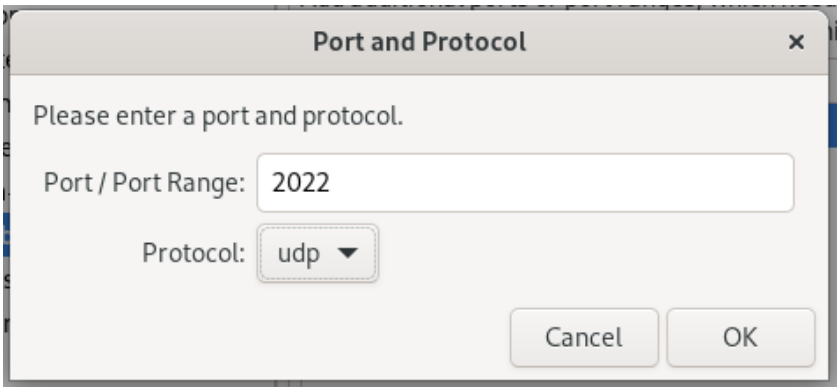

Рис. 3.24: Добавление порта

Закрываем утилиту firewall-config. В окне терминала вводим *firewall-cmd –list-all*. Изменения, которые мы только что внесли, ещё не вступили в силу. Это связано с тем, что мы настроили их как постоянные изменения, а не как изменения времени выполнения (рис. 3.25)

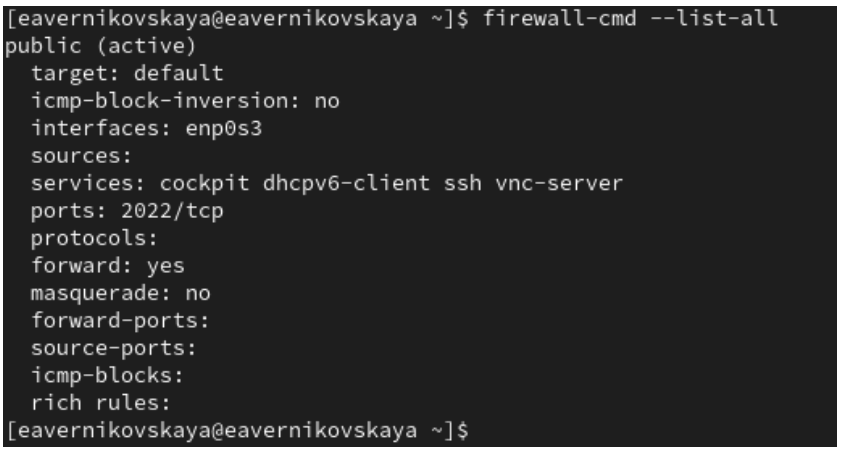

Рис. 3.25: Проверка внесённых изменений (1)

Перезагрузим конфигурацию firewall-cmd: *firewall-cmd –reload* (рис. 3.26)

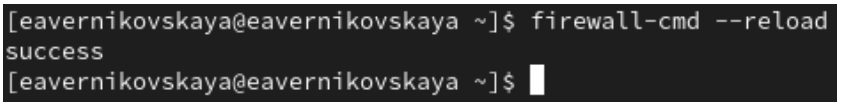

Рис. 3.26: Перезагрузка конфигурации firewall-cmd (1)

Снова проверяем список доступных сервисов. Мы видим, что изменения вступили в силу (рис. 3.27)

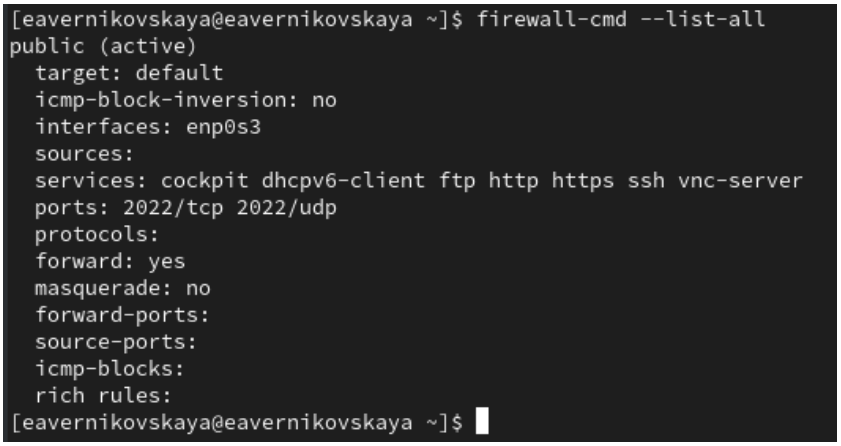

Рис. 3.27: Проверка внесённых изменений (2)

3.3 Самостоятельная работа

1. Надо создать конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам:

- telnet
- imap
- pop3
- smtp

2. Сделать это как в командной строке (для службы telnet), так и в графическом интерфейсе (для служб imap, pop3, smtp)

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

Сделаем службу telnet постоянной в командной строке: *firewall-cmd –add-service=telnet –permanent* (рис. 3.28)

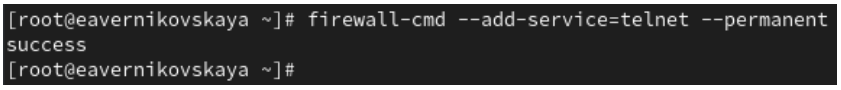

Рис. 3.28: Добавление постоянного telnet

Открываем интерфейс GUI firewall-config: *firewall-config* (рис. 3.29)

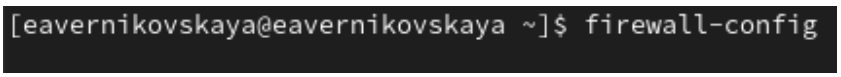

Рис. 3.29: Открытие интерфейса GUI firewall-config

Далее нажимаем выпадающее меню рядом с параметром Configuration. Открываем раскрывающийся список и выбираем Permanent. Выбираем зону public и отмечаем службы imap, pop3 и smtp, чтобы включить их (рис. 3.30)

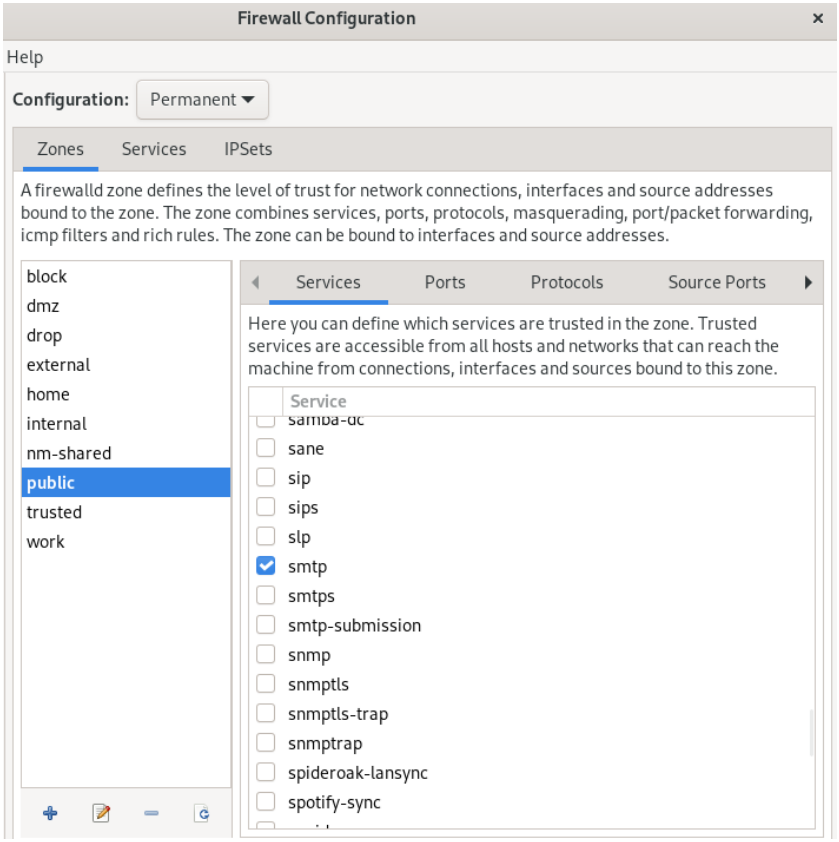

Рис. 3.30: Включение служб imap, pop3 и smtp

Перезагружаем конфигурацию firewall-cmd и проверсяем, что изменения были применены (рис. 3.31), (рис. 3.32)

```
[eavernikovskaya@eavernikovskaya ~]$ firewall-cmd --reload
success
[eavernikovskaya@eavernikovskaya ~]$
```

Рис. 3.31: Перезагрузка конфигурации firewall-cmd (2)

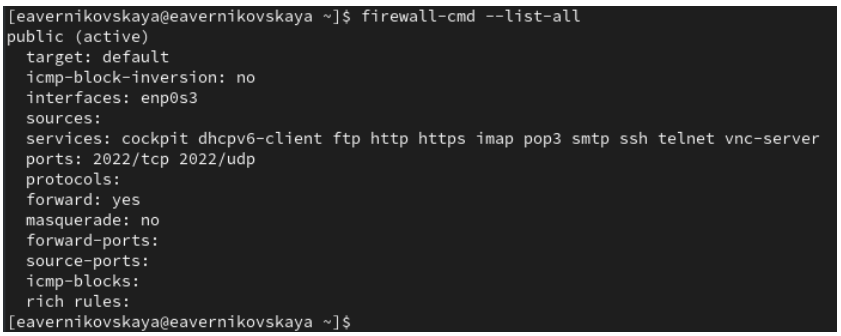

Рис. 3.32: Проверка внесённых изменений (3)

Далее убедимся, что конфигурация является постоянной и будет активирована после перезагрузки компьютера (рис. 3.33), (рис. 3.34)

Рис. 3.33: Перезагрузка ОС

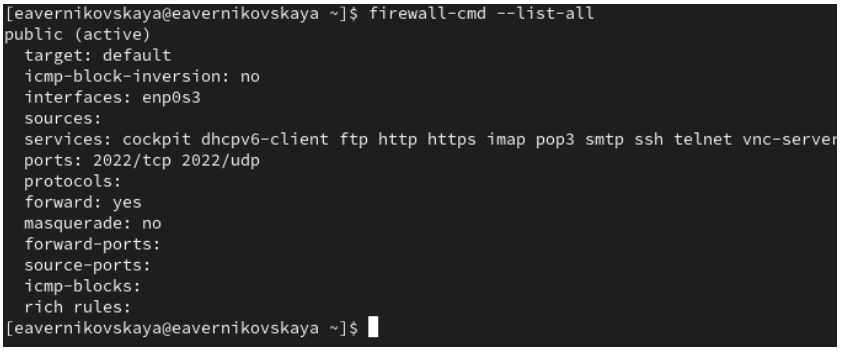

Рис. 3.34: Проверка внесённых изменений после перезагрузки ОС

4 Контрольные вопросы + ответы

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

sudo systemctl start firewalld

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

firewall-cmd –add-port=2355/udp –permanent

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

firewall-cmd –list-all-zones

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

firewall-cmd –remove-service=vnc-server

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

firewall-cmd –reload

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

firewall-cmd –list-all –zone=“zone-name”

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

firewall-cmd –zone=public –change-interface=eno1

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

В зону по умолчанию (firewall-cmd –get-default-zone)

5 Выводы

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

6 Список литературы

1. Лабораторая работа №13 [Электронный ресурс] URL: https://esystem.rudn.ru/pluginfile.php
   firewall.pdf