Лабораторная работа № 13. Фильтр пакетов

Дисциплина: Основы администрирования операционных систем

Жукова Арина Александровна

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: – добавьте службы http и ssh в зону public; – добавьте порт 2022 протокола UDP в зону public; – добавьте службу ftp.
3. Выполните задание для самостоятельной работы (раздел 13.5).

3 Выполнение лабораторной работы

3.1 Управление брандмауэром с помощью firewall-cmd

1. Определила текущую зону по умолчанию, используя `firewall-cmd --get-default-zone`. Определила доступные зоны `firewall-cmd --get-zones`. Посмотрела службы, доступные на моём компьютере, используя `firewall-cmd --get-services`. Определила доступные службы в текущей зоне `firewall-cmd --list-services` (рис. 3.1).

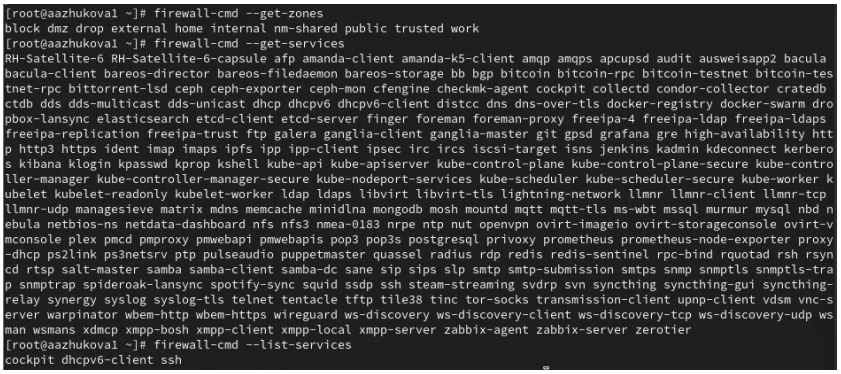

Рис. 3.1: Определение текущей зоны по умолчанию, доступной зоны, доступные службы на компьютере, доступные зоны в текущей зоне

2. Сравнила результаты вывода информации при использовании команды `firewall-cmd --list-all` и `firewall-cmd --list-all --zone=public` (рис. 3.2).

```
[root@aazhukova1 ~]# 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@aazhukova1 ~]# firewall-cmd --list-all --zone=public
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@aazhukova1 ~]#
```

Рис. 3.2: Результаты вывода двух команд

3. Добавила сервер VNC в конфигурацию брандмауэра `firewall-cmd --add-service=vnc-server`. Проверила, добавился ли vnc-server в конфигурацию (рис. 3.3).

```
[root@aazhukova1 ~]# firewall-cmd --add-service=vnc-server
success
[root@aazhukova1 ~]# 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:
```

Рис. 3.3: Добавление VNC сервера

4. Перезапустила службу firewalld. Проверила, есть ли vnc-server в конфигурации. (рис. 3.4).

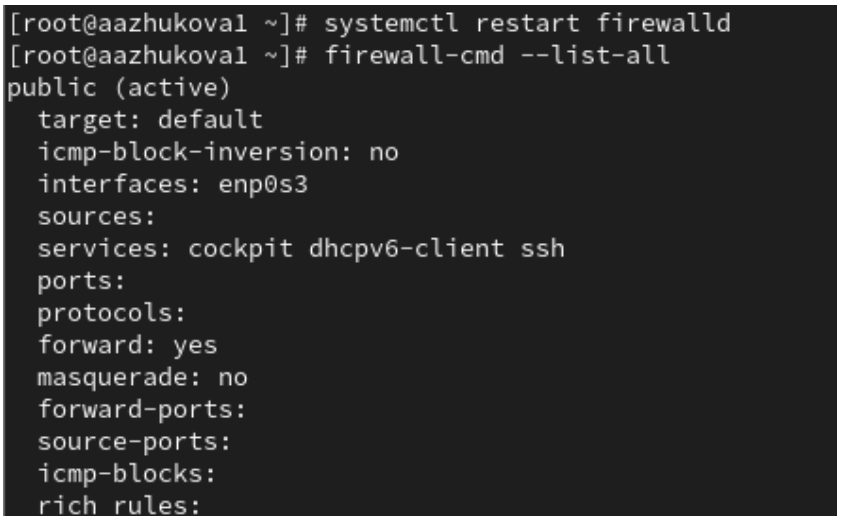

Рис. 3.4: Перезапуск службы, проверка наличия сервера

Служба vnc-server больше не указана, так как была не постоянной.

5. Добавила службу vnc-server ещё раз, но на этот раз сделала её постоянной, проверила наличие vnc-server в конфигурации (рис. 3.5).

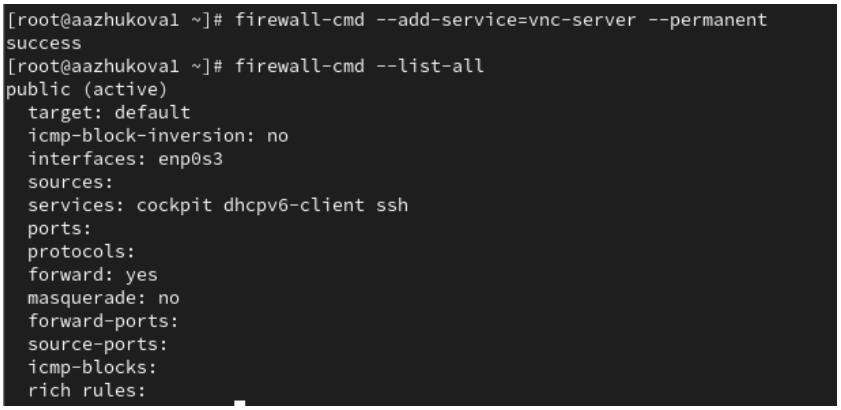

Рис. 3.5: Добавление постоянной службы vnc-server

Я увидела, что VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения.

6. Перезагрузила конфигурацию firewalld и просмотрела конфигурацию времени выполнения (рис. 3.6).

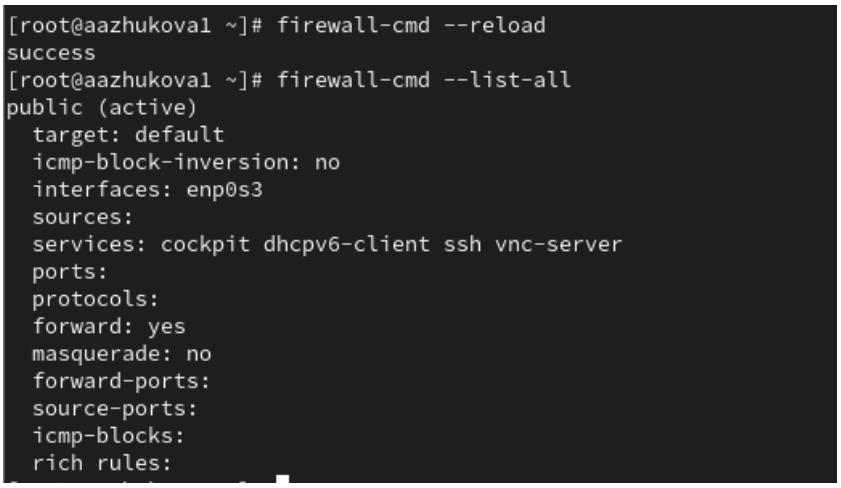

Рис. 3.6: Перезагрузка конфигурации

7. Добавила в конфигурацию межсетевого экрана порт 2022 протокола TCP, затем перезагрузила конфигурацию firewalld `firewall-cmd --reload`, проверила, что порт добавлен в конфигурацию (рис. 3.7).

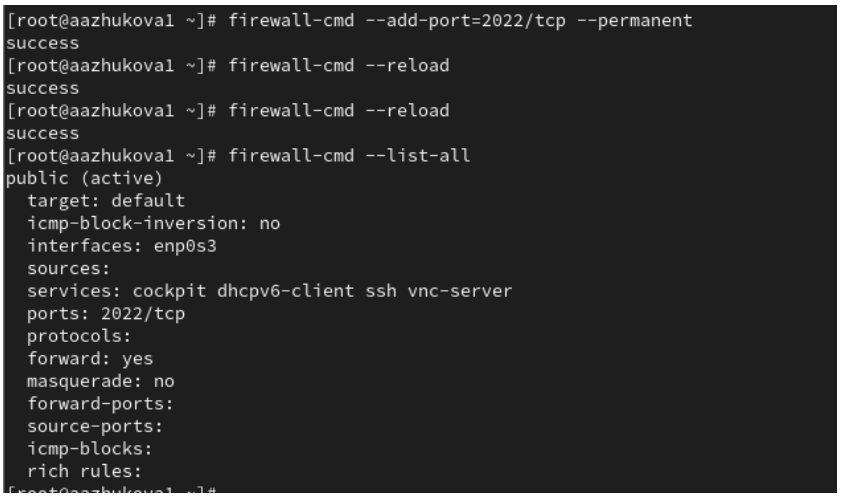

Рис. 3.7: Добавление межсетевого экрана, перезагрузка конфигурации

3.2 Управление брандмауэром с помощью firewall-config

1. Открыла терминал и под учётной записью своего пользователя запустила интерфейс GUI firewall-config. Нажала выпадающее меню рядом с параметром Configuration. Открыла раскрывающийся список и выбрала Permanent. Выбрала зону public и отметила службы http, https и ftp, чтобы включить их (рис. 3.8).

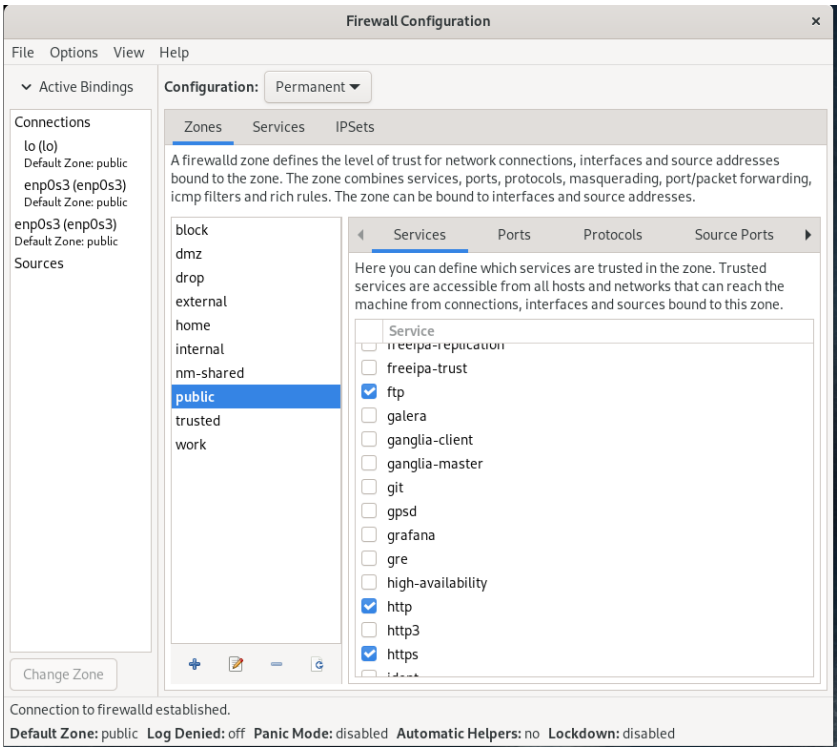

Рис. 3.8: Интерфейс GUI firewall-config

2. Выбрала вкладку Ports и на этой вкладке нажала Add. Ввела порт 2022 и протокол udp, нажала ОК, чтобы добавить их в список (рис. 3.9).

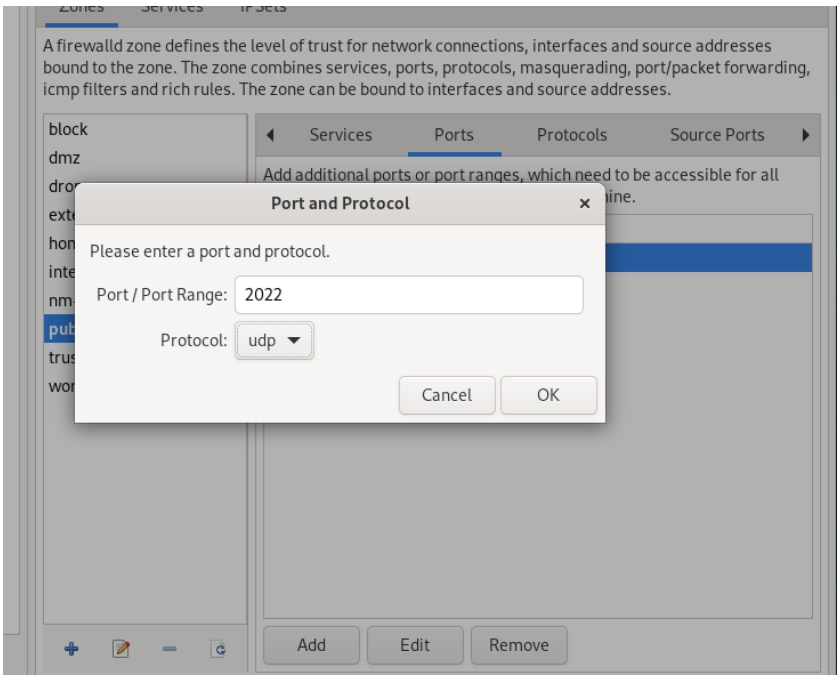

Рис. 3.9: Добавление нового порта

Закрыла утилиту firewall-config.

3. Просмотрела список доступных серверов, перезагрузила конфигурацию firewall-cmd и снова просмотрела список доступных сервисов (рис. 3.10).

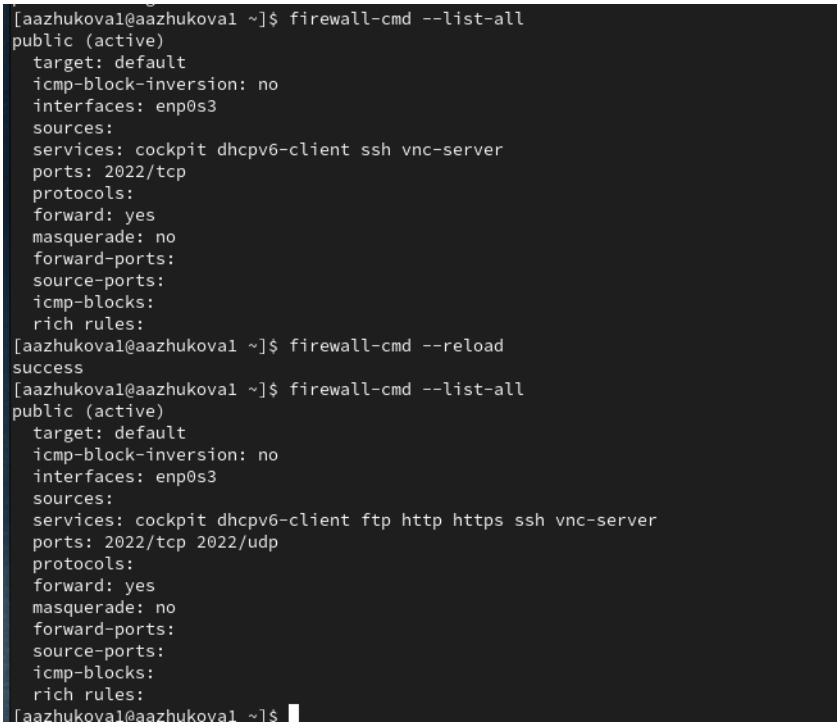

Рис. 3.10: Проверка подключения серверов

3.3 Самостоятельная работа

1. Добавление службы telnet в конфигурацию через терминал. (рис. 3.11).

Рис. 3.11: Добавление службы telnet

2. Создала конфигурацию межсетевого экрана, которая позволяет получить доступ к imap, pop3, smtp в графическом интерфейсе (рис. 3.12).

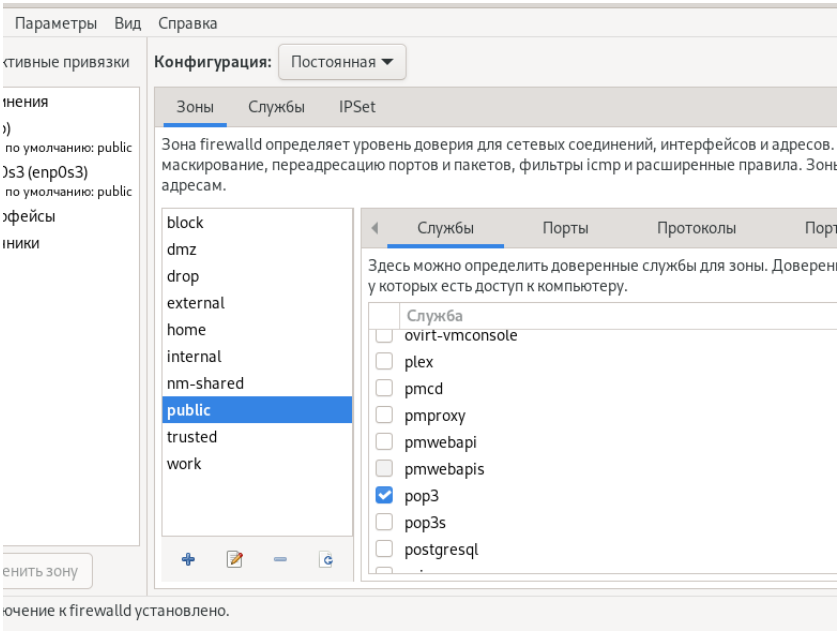

Рис. 3.12: Добавление через графический интерфейс

3. Убедилась, что конфигурация является постоянной и будет активирована после перезагрузки компьютера (рис. 3.13).

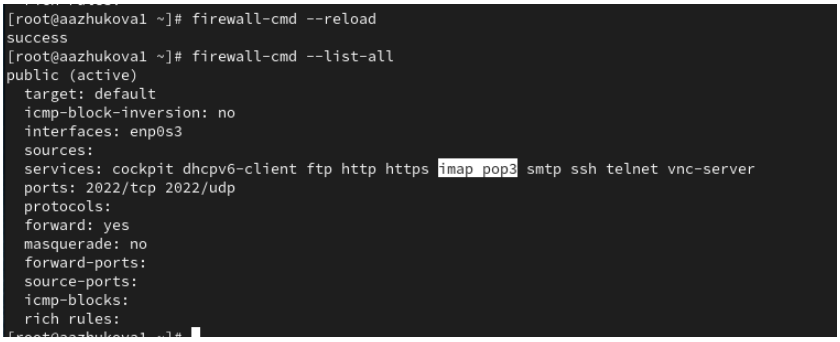

Рис. 3.13: Проверка добавления

4 Выводы

В ходе выполнения лабораторной работы получила навыки настройки пакетного фильтра в Linux.

Список литературы

1. Purdy G. N. Linux iptables Pocket Reference. — O'Reilly Media, 2004. — (Pocket Reference).
2. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб. : БХВПетербург, 2011. — (Системный администратор).
3. Vugt S. van. Red Hat RHCSA/RHCE 7 cert guide : Red Hat Enterprise Linux 7 (EX200 and EX300). — Pearson IT Certification, 2016. — (Certification Guide).
4. Динамический брандмауэр с использованием FirewallD. — URL: https : / / fedoraproject.org/wiki/FirewallD/ru.