Фильтр пакетов

Лабораторная работа №13

Казначеев С.И.

25 ноября 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

::::::::::::::: {.columns align=center} ::: {.column width="70%"}

- Казначеев Сергей Ильич
- Студент
- Российский университет дружбы народов
- [1132240693@pfur.ru] ::: ::: {.column width="30%"}

Цель работы

Получить навыки настройки пакетного фильтра в Linux.

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).

Перейдем в супер пользователя

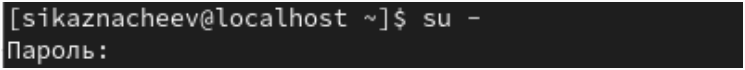

Рис. 1: 1

После чего определим текущую зону

```
[root@localhost ~]# firewall-cmd --get-default-zone
public
```

Рис. 2: 2

Определение доступной зоны

Определим доступные зоны

```
[root@localhost ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
```

Рис. 3: 3

Просмотр служб на нашем компьютере

Затем просмотрим службы доступные на нашем компьютере

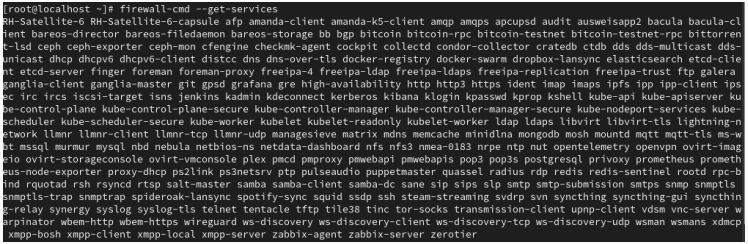

Рис. 4: 4

Определяем доступные службы

Определим доступные службы в текущей зоне

```
[root@localhost ~]# firewall-cmd --list-services
cockpit dhcpv6-client ssh
```

Рис. 5: 5

Сравнение двух команд

После чего сравним вывод информации при использовании двух команд первая команда firewall-cmd –list-all,вторая firewall-cmd –list-all –zone=public

```
[root@localhost ~]# 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@localhost ~]# irewall-cmd --list-all --zone=public
bash: irewall-cmd: команда не найдена...
[root@localhost ~]# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
```

Добавление сервера VNC

Далее добавим сервер VNC в конфигурацию брандмауэра

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

Рис. 7: 7

И проверим добавился или нет

```
[root@localhost ~]# 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. 8: 8

Запуск службы firewalld

После чего перезапустим службу firewalld

```
[root@localhost ~]# systemctl restart firewalld
```

Рис. 9: 9

Проверка vnc-server в конфигурации

Затем проверим есть ли vnc-server в конфигурации и мы обнаружим,что vnc-server больше не указан это из за того что не был постоянным

```
[root@localhost ~]# 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:
```

Рис. 10: 10

Добавление службы vnc-server только уже постоянной

Добавим службу vnc-server ещё раз, но на этот раз сделав её постоянной

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

Рис. 11: 11

Проверка vnc-server в конфигурации

После чего проверим наличие vnc-server в конфигурации

```
[root@localhost ~]# 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:
```

Проверка vnc-server после перезагрузки firewalld

Теперь проверим перезагрузив конфигурацию firewalld

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

Добавление конфигурации межсетевого экрана

Добавим в конфигурацию межсетевого экрана порт 2022 протокола TCP,после чего перезагрузим конфигурацию firewalld и прроверим что порт добавился в конфигурацию

```
[root@localhost ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# firewall-cmd --list-all
public (active)
  target: default
  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:
```

Рис. 14: 14

Запускт интерфейса GUI firewall-config

После чего откроем терминал и под учетной записью пользователя запустим интерфейс GUI firewall-config

```
[sikaznacheev@localhost ~]$ firewall-config
```

Рис. 15: 15

Далее рядом с параметром Configuration откроем раскрывающийся список и выберем Permanent, после чего выберем зону public и отметим службы http, https и ftp

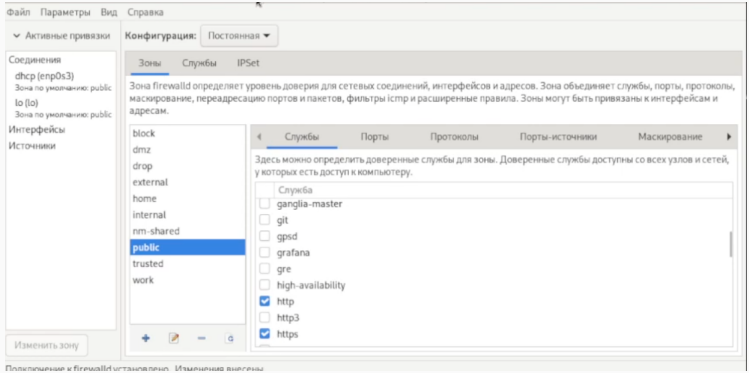

Рис. 16: 16

Рис. 17: 17

Добавление порта через GUI firewall-config

Полче чего выберем вкладку Ports и добавим порт 2022 udp

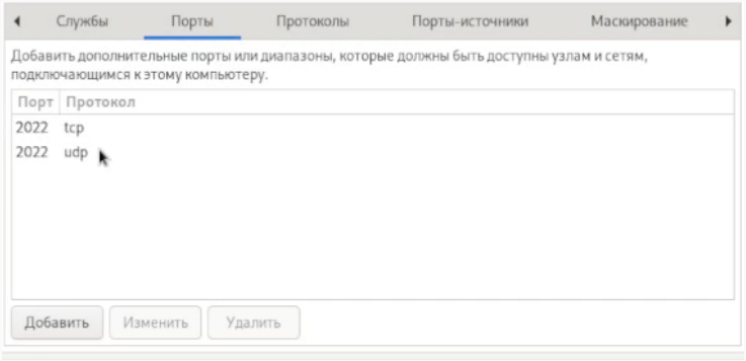

Рис. 18: 18

Проверка всех изменений

И проверим все изменения которые мы только что внесли

```
[sikaznacheev@localhost ~]$ firewall-cmd --list-all
public (active)
  target: default
  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:
```

Рис. 19: 19

Перезапуск конфигурации firewall-cmd

Перезапустим конфигурацию firewall-cmd для того,чтобы изменения вступили в силу и проверим это

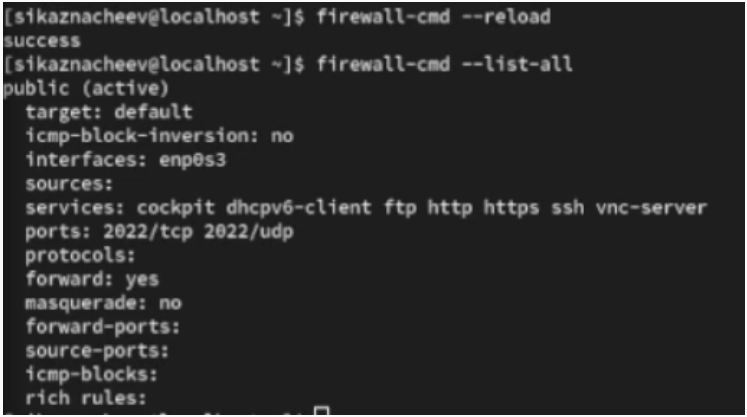

Рис. 20: 20

Создадим конфигурацию межсетевого экрана которая позволяет получить доступ к следующим службам telnet,imap, pop3, smtp

Рис. 21: 21

Добавляем imap, pop3, smtp

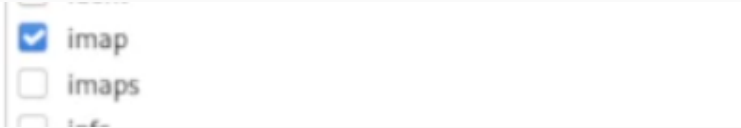

Рис. 22: 22

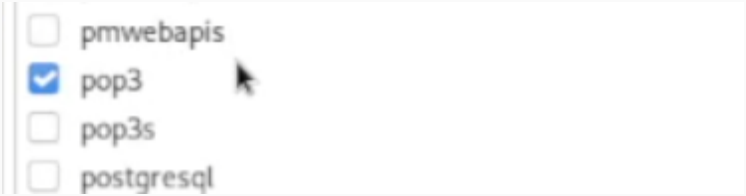

Рис. 23: 23

Рис. 24: 24

Проверка что конфигурация является постоянной

И проверяем,что конфигурация является постоянной и будет активирована после перезагрузки компьютера

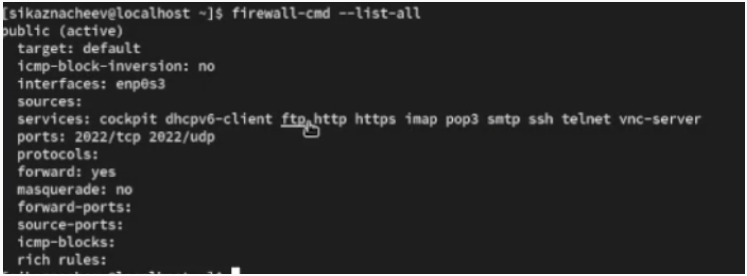

Рис. 25: 25

Контрольные вопрос 1

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

Ответ - firewall должна быть запущена

Контрольные вопрос 2

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

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

Контрольные вопрос 3

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

Ответ - firewall-cmd –list-all-zones

Контрольные вопрос 4

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

Ответ - firewall-cmd –remove-service=vnc-server

Контрольные вопрос 5

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

Ответ - firewall-cmd –reload

Контрольные вопрос 6

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

Ответ - firewall-cmd –list-all

Контрольные вопрос 7

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

Ответ - firewall-cmd –zone=public –add-interface=eno1

Контрольные вопрос 8

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

Ответ - интерфейс попадет в зону по умолчанию (public)

Выводы

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