Фильтр пакетов

Отчет

Казначеев Сергей Ильич

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

Перейдем в супер пользователя

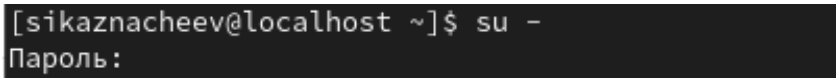

Рис. 3.1: 1

После чего определим текущую зону

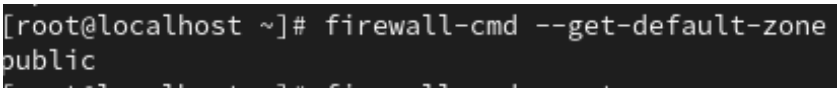

Рис. 3.2: 2

Определим доступные зоны

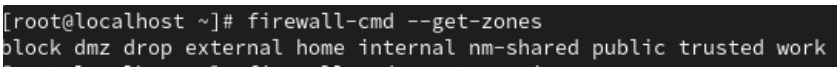

Рис. 3.3: 3

Затем просмотрим службы доступные на нашем компьютере

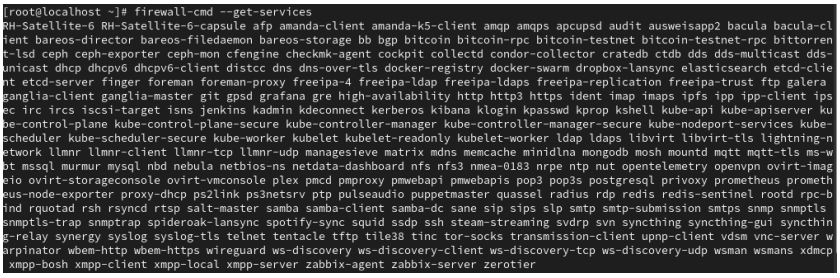

Рис. 3.4: 4

Определим доступные службы в текущей зоне

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

Рис. 3.5: 5

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:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 3.6: 6

Далее добавим сервер VNC в конфигурацию брандмауэра

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

Рис. 3.7: 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. 3.8: 8

После чего перезапустим службу firewalld

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

Рис. 3.9: 9

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. 3.10: 10

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

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

Рис. 3.11: 11

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:
```

Рис. 3.12: 12

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:
```

Рис. 3.13: 13

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. 3.14: 14

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

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

Рис. 3.15: 15

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

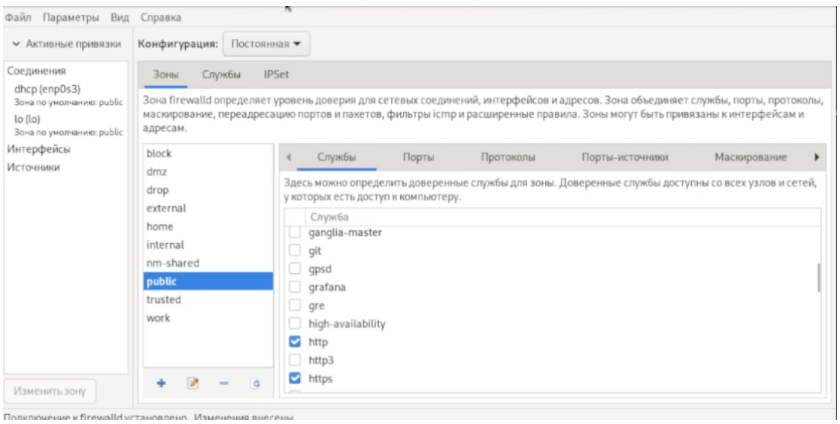

Рис. 3.16: 16

Рис. 3.17: 17

Полче чего выберем вкладку Ports и добавим порт 2022 udp

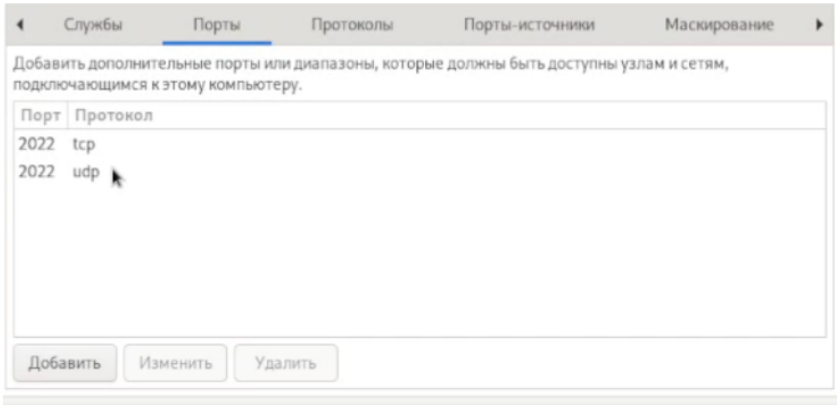

Рис. 3.18: 18

И проверим все изменения которые мы только что внесли

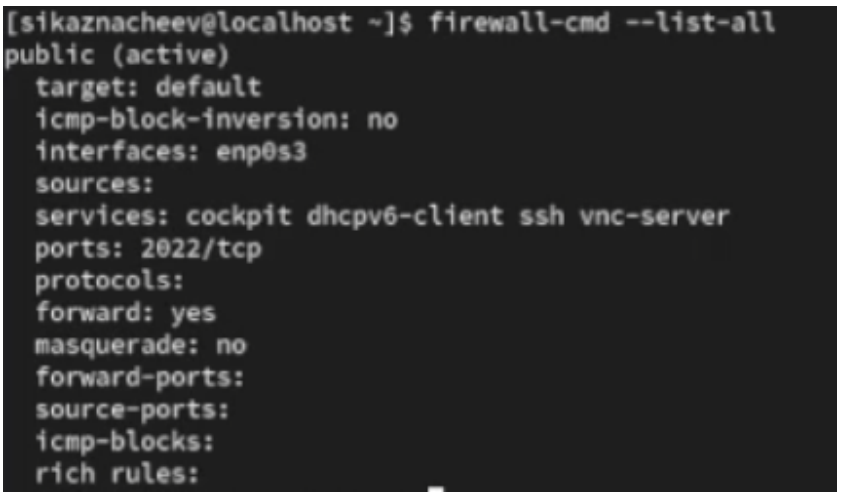

Рис. 3.19: 19

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

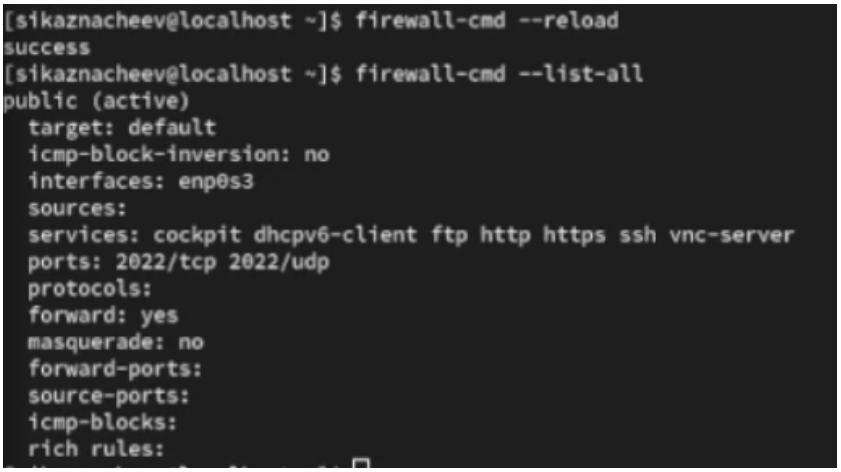

Рис. 3.20: 20

4 Самостоятельная работа

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

```
[sikaznacheev@localhost ~]$ firewall-cmd --add-service=telnet --permanent
success
```

Рис. 4.1: 21

Добавляем imap, pop3, smtp

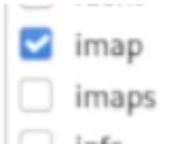

Рис. 4.2: 22

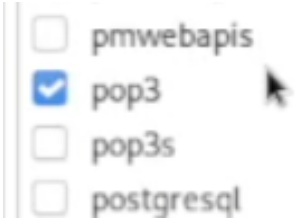

Рис. 4.3: 23

Рис. 4.4: 24

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

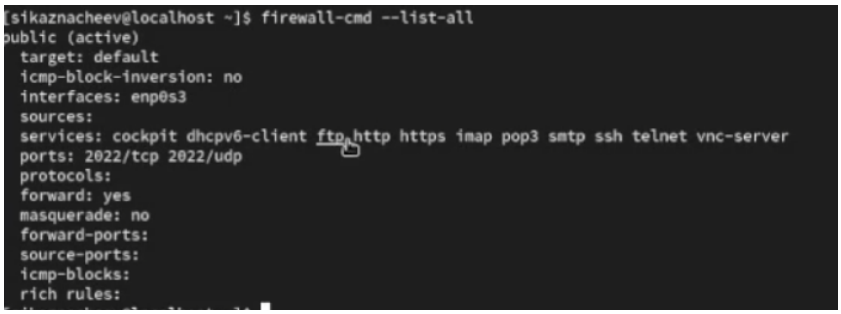

Рис. 4.5: 25

5 Контрольные вопросы

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

Ответ - firewall должна быть запущена

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

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

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

Ответ - firewall-cmd –list-all-zones

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

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

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

Ответ - firewall-cmd –reload

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

Ответ - firewall-cmd –list-all

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

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

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)

6 Выводы

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