Фильтр пакетов

Майоров Дмитрий Андреевич

Содержание i

1. Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2. Выполнение лабораторной работы

Определяем текущую зону по умолчанию.Определяем доступные зоны. Смотрим службы, доступные на нашем компьютере

```
root@mayorovda:~# firewall-cmd --get-default-zone
public
root@mayorovda:~# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@mayorovda:~# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-
k5-client amqp amqps anno-1602 anno-1800 apcupsd aseqnet audit ausweisapp
```

Рисунок 1

Определяем доступные службы в текущей зоне

```
root@mayorovda:~# firewall-cmd --list-services
cockpit dhcpv6-client ssh
```

Рисунок 2

4. Выполнение лабораторной работы

Вводим следующие команды. Первая показывает реальное состояние активной зоны с учетом всех примененных правил и привязанных интерфейсов. Вторая показывает конфигурацию зоны как она хранится в памяти, включая все настройки

```
root@mayorovda:~# firewall-cmd --list-all
public (default, active)
  target: default
```

Рисунок 3

```
root@mayorovda:~# firewall-cmd --list-all --zone=public
public (default, active)
  target: default
  ingress-priority: 0
```

Рисунок 4

5. Выполнение лабораторной работы

Добавляем сервер VNC в конфигурацию брандмауэра. Проверяем, добавился ли vnc-server в конфигурацию

```
root@mayorovda:~# firewall-cmd --add-service=vnc-server
success
root@mayorovda:~# 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
```

Рисунок 5

6. Выполнение лабораторной работы

Перезапускаем службу firewalld. Проверяем, есть ли vnc-server в конфигурации. Его больше нет, так как мы добавляли его без команды permanent

```
root@mayorovda:~# systemctl restart firewalld
root@mayorovda:~# 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
```

Рисунок 6

7. Выполнение лабораторной работы

Добавляем службу vnc-server ещё раз, но на этот раз делаем её постоянной

```
root@mayorovda:~# firewall-cmd --add-service=vnc-server --permanent
success
root@mayorovda:~# 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
```

Рисунок 7

8. Выполнение лабораторной работы

Перезагружаем конфигурацию firewalld и смотрим конфигурацию времени выполнения

```
root@mayorovda:~# firewall-cmd --reload
success
root@mayorovda:~# 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
```

Рисунок 8

9. Выполнение лабораторной работы

Добавляем в конфигурацию межсетевого экрана порт 2022 протокола TCP. Перезагружаем конфигурацию firewalld. Проверяем, что порт добавлен в конфигурацию

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

Рисунок 9

```
sources:
services: cockpit dhcpv6-client ssh vnc-server
ports: 2022/tcp
protocols:
```

Рисунок 10

10. Выполнение лабораторной работы

Устанавливаем интерфейс GUI firewall-config

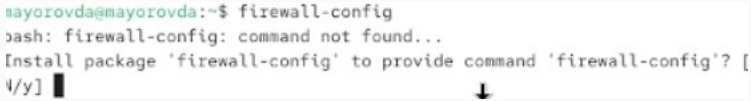
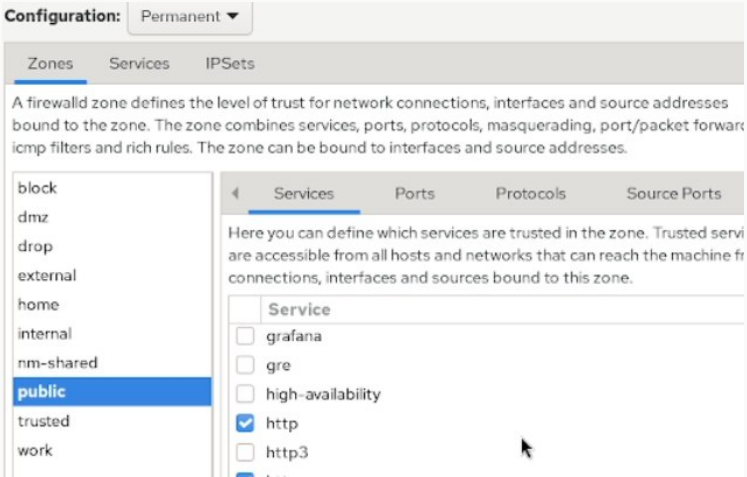


Рисунок 11

11. Выполнение лабораторной работы

При запуске службы вводим пароль. Выбираем опцию Permanent. Отмечаем нужные нам службы



Вводим порт 2022 и протокол udp. Добавляем их в список

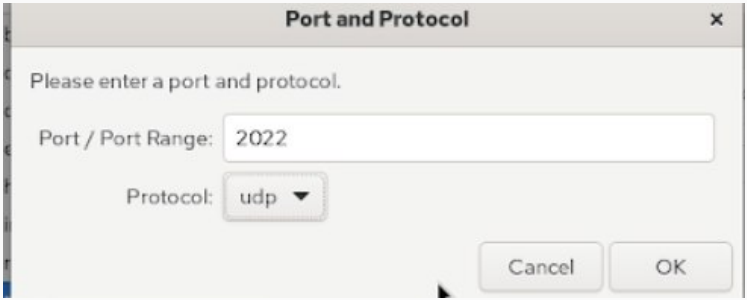


Рисунок 13

13. Выполнение лабораторной работы

Перезагружаем конфигурацию firewall-cmd. Смотрим конфигурацию. Видим что изменения применены

```
root@mayorovda:~# 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
```

Рисунок 14

14. Самостоятельная работа

Добавляем службу telmet, делаем ее постоянной. Перезагружаем конфигурацию firewall-cmd. Смотрим конфигурацию

```
root@mayorovda:~# firewall-cmd --add-service=telnet --permanen
success
root@mayorovda:~# irewall-cmd --reload
bash: irewall-cmd: command not found...
irewall-cmd --reloadroot@mayorovda:~# firewall-cmd --reload
success
```

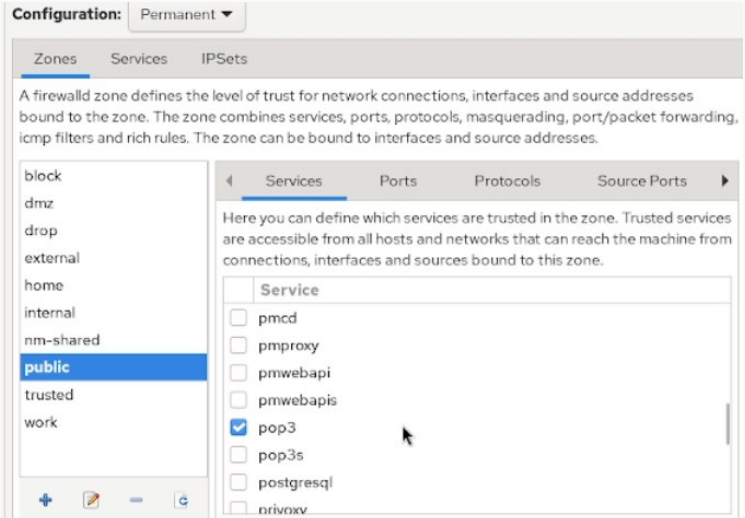
Рисунок 15

```
sources:
services: cockpit dhcpv6-client ftp http https ssh telnet vnc-server
ports: 2022/tcp 2022/udp
```

Рисунок 16

15. Самостоятельная работа

Добавляем нужные нам службы через графический интерфейс



16. Самостоятельная работа

Проверяем, что службы добавлены в конфигурацию

Рисунок 18

17. Выводы

Получены навыки настройки пакетного фильтра в Linux.