

Отчёт по лабораторной работе 13

Фильтр пакетов

Вишняков Родион Сергеевич

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
3 Вывод	14
4 Контрольные вопросы	15

Список иллюстраций

2.1	Службы	6
2.2	Сравнение	7
2.3	vnc-server	8
2.4	Постоянная служба	9
2.5	Порт	10
2.6	Графический интерфейс	10
2.7	Графический интерфейс	11
2.8	Службы и порт	12
2.9	Самостоятельная работа	13

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2 Выполнение лабораторной работы

Получаем полномочия администратора, определяем текущую зону по умолчанию, определяем доступные зоны, смотрим службы доступные на вашем компьютере, определяем доступные службы в текущей зоне.

```
rodvish@vbox:~$ sudo -i
[sudo] пароль для rodvish:
root@vbox:~# firewall-cmd --get-default-zone
public
root@vbox:~# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@vbox:~# firewall-cmd --list-services
cockpit dhcpcv6-client ssh
```

Рис. 2.1: Службы

Сравниваем результаты вывода информации

```
root@vbox:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
    services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@vbox:~# firewall-cmd --list-all --zone=public
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
    services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@vbox:~#
```

Рис. 2.2: Сравнение

Добавил сервер VNC в конфигурацию брандмауэра, проверил добавился ли vnc-server в конфигурацию, перезапустил службу firewalld, проверил есть ли vnc-server в конфигурации

```
root@vbox:~# firewall-cmd --add-service=vnc-server
success
root@vbox:~# firewall-cmd --list-all
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page
firewall-cmd: error: ambiguous option: --list-all could match --list-all-zones, --list-all-policies, --list-all
root@vbox:~# 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
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@vbox:~# systemctl restart firewalld
root@vbox:~# 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
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
```

Рис. 2.3: vnc-server

Добавили службу vns-server и сделали ее постоянной, проверили наличие службы, перезагрузили конфигурацию firewalld, и просмотрели конфигурацию времени выполнения

```
root@vbox:~# firewall-cmd --add-service=vnc-server --permanent
success
root@vbox:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
    services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@vbox:~# firewall-cmd --reload
success
root@vbox:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
    services: cockpit dhcpcv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@vbox:~#
```

Рис. 2.4: Постоянная служба

Добавили в конфигурацию межсетевого экрана порт 2022 протокола TCP, перезагрузили конфигурацию firewalld, проверили что порт добавлен в конфигурацию

```

root@vbox:~# firewall-cmd --add-port=2022/tcp --permanent
success
root@vbox:~# firewall-cmd --reload
success
root@vbox:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
    services: cockpit dhcpcv6-client ssh vnc-server
    ports: 2022/tcp
    protocols:
      forward: yes
      masquerade: no
    forward-ports:
    source-ports:
    icmp-blocks:
    rich rules:
root@vbox:~#

```

Рис. 2.5: Порт

Запустили графический интерфейс и включили http, https и ftp службы

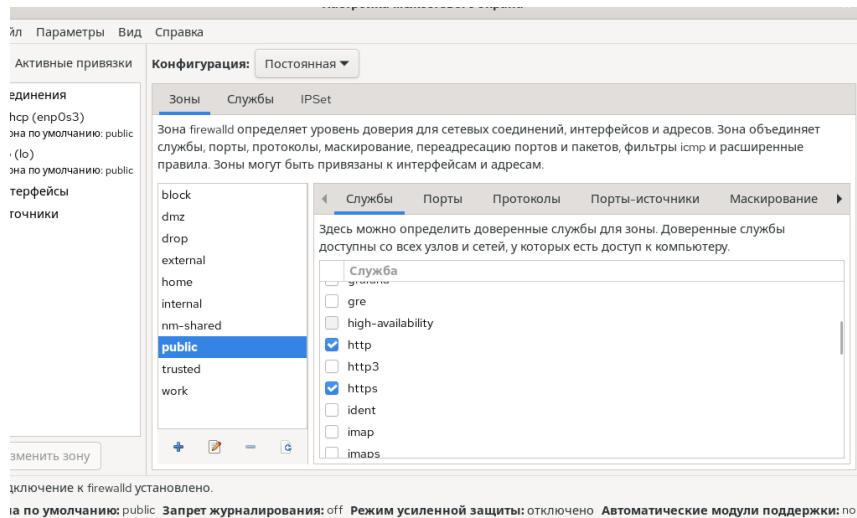


Рис. 2.6: Графический интерфейс

Добавили новый порт в список

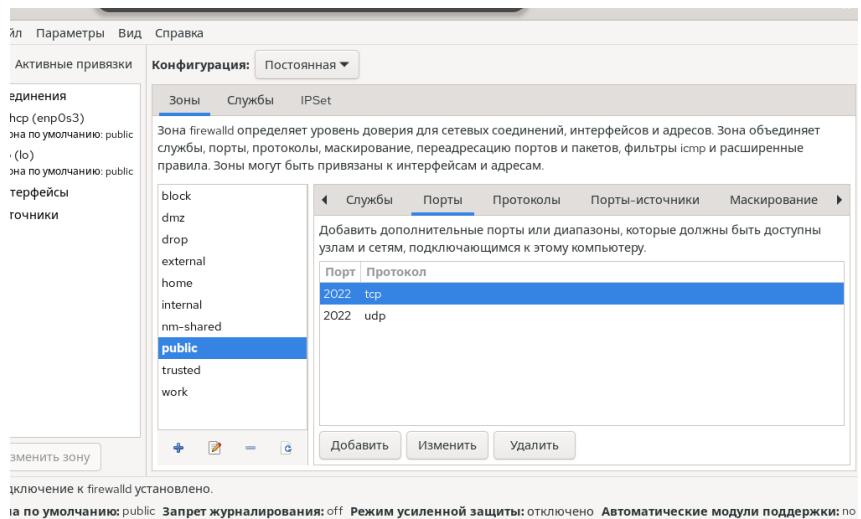


Рис. 2.7: Графический интерфейс

Перегрузил конфигурацию firewall-cmd и проверил новые добавления

```
rodvish@vbox:~$ firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
    services: cockpit dhcpcv6-client ssh vnc-server
    ports: 2022/tcp
    protocols:
      forward: yes
      masquerade: no
      forward-ports:
      source-ports:
      icmp-blocks:
      rich rules:
rodvish@vbox:~$ firewall-cmd --reload
success
rodvish@vbox:~$ firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
    services: cockpit dhcpcv6-client ftp http https ssh vnc-server
    ports: 2022/tcp 2022/udp
    protocols:
      forward: yes
      masquerade: no
      forward-ports:
      source-ports:
      icmp-blocks:
      rich rules:
rodvish@vbox:~$
```

Рис. 2.8: Службы и порт

Проделал задание для самостоятельной работы

```
rodvish@vbox:~$ firewall-cmd --add-service=telnet --permanent
success
rodvish@vbox:~$ firewall-cmd --reload
success
rodvish@vbox:~$ firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ftp http https ssh telnet vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
rodvish@vbox:~$ firewall-config
rodvish@vbox:~$ firewall-cmd --reload
success
rodvish@vbox:~$ firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ftp http https imap pop3 smtp ssh telnet vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
rodvish@vbox:~$ █
```

Рис. 2.9: Самостоятельная работа

3 Вывод

Мы получили навыки настройки пакетного фильтра в Linux.

4 Контрольные вопросы

1. Вопрос: Какая служба должна быть запущена перед началом работы с менеджером конфигурации брандмауэра firewall-config? Ответ: Служба firewalld.
2. Вопрос: Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию? Ответ: Команда firewall-cmd –add-port=2355/udp.
3. Вопрос: Какая команда позволяет показать всю конфигурацию брандмауэра во всех зонах? Ответ: Команда firewall-cmd –list-all-zones.
4. Вопрос: Какая команда позволяет удалить службу vnc-server из текущей конфигурации брандмауэра? Ответ: Команда firewall-cmd –remove-service=vnc-server.
5. Вопрос: Какая команда firewall-cmd позволяет активировать новую конфигурацию, добавленную опцией –permanent? Ответ: Команда firewall-cmd –reload.
6. Вопрос: Какой параметр firewall-cmd позволяет проверить, что новая конфигурация была добавлена в текущую зону и теперь активна? Ответ: Параметр –list-all.
7. Вопрос: Какая команда позволяет добавить интерфейс eno1 в зону public? Ответ: Команда firewall-cmd –zone=public –add-interface=eno1.
8. Вопрос: Если добавить новый интерфейс в конфигурацию брандмауэра, пока не указана зона, в какую зону он будет добавлен? Ответ: В зону по умолчанию default zone.